TUTTO QUELLO CHE GLI ALTRI NON DICONO

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€

HACKER JOURNAL

n. 191

www.hackerjournal.it

TV SATELLITARE
SKY CONDIVISO



SCUOLA HACKER
LA SCANSIONE DELLE PORTE

SECURITY
CYBERWAR UN RISCHIO REALE

GAMES
A CACCIA DI LADRI INTERNET EYE

FOCUS ON
THE PIRATE BAY RINASCE CON IL TRUCCO

QUATTORD. ANNO 09 - N° 191 - 17 DICEMBRE 2009/6 GENNAIO 2010 - € 2,00

WLF PUBLISHING

Anno 09 - N.191
17 dicembre 2009 / 6 gennaio 2010

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

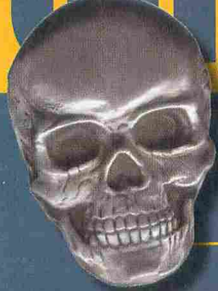
HACKER JOURNAL
Pubblicazione quattordicinale registrata
al Tribunale di Milano
il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



HJ hackerato

"Due cose sono infinite: l'universo e la stupidità umana, ma riguardo l'universo ho ancora dei dubbi."
(Albert Einstein)

Ebbene sì siamo stati hackerati.

La storia è semplice, sfruttando un bug del forum qualcuno ha pensato di fare piazza pulita di tutto quanto si trovava su server che ci ospitava e sulle prime ci si potrebbero fare anche delle grasse risate: proprio a noi!

La storiella però è meno divertente se si va un po' più a fondo.
Da quando Hacker Journal è nato abbiamo dedicato tutto il nostro impegno e la nostra passione per far passare un concetto tanto chiaro quanto semplice: essere hacker significa voler scoprire cosa c'è dietro alle cose, significa non fermarsi all'apparenza, significa condividere la propria conoscenza. Essere hacker non significa usare le proprie conoscenze per danneggiare gli altri.

Lo abbiamo ripetuto in mille modi, non tutti hanno capito.

Hacker Journal è un quindicinale che da tanti anni esce solo grazie all'impegno di un editore che ha scelto di dedicarsi a questa avventura per passione, non certo per business (2€ senza mezza pagina di pubblicità). Un editore che ha investito tempo e danaro per consentire la nascita e lo sviluppo di una community (il Forum) dove tutti potessero esprimersi liberamente.

E ciò che davvero ferisce è la provenienza di questo attacco: "vogliamo il vecchio forum"... Cioè uno di noi!
È difficile spiegare la sensazione che si prova quando a colpirti alle spalle è un amico, viene (quasi) voglia di mollare, lasciare tutto e pensare ad altro.

Quasi, appunto.

Andiamo avanti con l'entusiasmo di sempre, cercando di fare un Hacker Journal sempre migliore, con l'aiuto di chi crede davvero nella nostra idea di hacker, con chi vorrà condividere con noi il proprio entusiasmo e voglia di conoscenza, con chi vorrà aiutarci a far crescere il nostro giornale.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ: mandateci una mail!
Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa.
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Quando l'hacking diventa business

La notizia è destinata ad avvalorare quella leggenda metropolitana, ma in realtà neppure tanto leggenda, dell'hacker che dopo aver dimostrato la propria "bravura" craccando, hackerando e via dicendo, viene assunto dalla nota industria come super esperto e diventa immensamente ricco. Nella fattispecie il caso arriva dall'Australia dove Ashley Towns, lo sviluppatore di ikee ovvero il primo worm capace di attaccare gli iPhone con jailbreak (la procedura che "libera" i dispositivi dai vincoli di Apple per installare software libero), è stato assunto dall'azienda Moogeneration in qualità di sviluppatore di applicazioni per iPhone.



Non è la prima volta che succede e non sarà l'ultima: l'inventore del worm Anna Kournikova fu assunto come esperto IT dall'amministrazione della cittadina olandese di Sneek o ancora lo sviluppatore dei worm Netsky e Sasser, tra i più dannosi della storia della Rete, venne assunto, sempre in qualità di esperto IT, da un'azienda tedesca.

E anche oggi, come per le volte precedenti, viene da chiedersi: e l'etica dove la mettiamo? Non stiamo parlando di piccole bravate, "simpatiche intrusioni" in un social network per rubare pettegolezzi. Creare e diffondere un worm significa creare ingenti danni a migliaia di persone, significa, in poche parole, commettere un crimine. Qualcuno potrebbe obiettare che nel caso specifico ikee si limitava a sostituire lo sfondo degli iPhone attaccati con l'immagine di Rick Astley, una pop star degli Anni '80 che pochi ricordano. Non faceva danni. Vero solo in parte, perché il codice sorgente di ikee è stato successivamente sviluppato per dare vita a nuovi virus decisamente più pericolosi per le vittime.

Abbiamo mai sentito di un rapinatore che viene assunto da una banca come guardia giurata? Di un finanziere senza scrupoli che dopo aver truffato migliaia di persone diventa collaboratore della Guardia Finanza? Certo che no. È un po' come la storia delle autoradio: in quanti ne hanno comprata una a buon prezzo, ben sapendo che chi gliela vendeva non aveva "lo scontrino" senza farsi troppe domande per poi infuriarsi quando il giorno dopo si trovavano il vetro dell'auto in frantumi e l'autoradio "usata" era sparita?

Ognuno è responsabile delle proprie azioni, soprattutto quando *queste* coinvolgono *migliaia*, se non milioni, di altre persone.

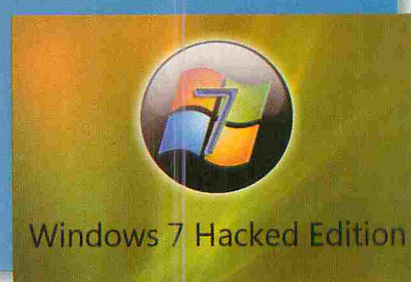
SMARTPHONE LETALE?

Secondo Scott Totzke, vicepresidente della sicurezza a BlackBerry di RIM, gli hacker potrebbero un giorno dedicarsi a trasformare gli smartphone in apparecchi capaci di intrusioni, per attaccare le reti wireless. Per prendere di mira gli operatori di telefonia mobile gli hacker potrebbero utilizzare la già sperimentata tecnica dei segnali telefonici che ordinano a migliaia di computer di contattare ripetutamente un sito, rallentandolo o facendolo crollare. La tecnica comprenderebbe pacchetti di dati che possono essere utilizzati per far cadere una rete wireless, anche se gli hacker possano raggiungere tale scopo usando un numero piuttosto limitato di smartphone. I software malevoli in grado di realizzare queste intrusioni potrebbero venire da applicazioni che gli utilizzatori di smartphone installano ignari di installare e versioni con virus di applicazioni diffuse e innocue (se scaricate dai siti ufficiali).



UNA PROTEZIONE CON I BUCHI

È ufficiale: l'attivazione di Windows 7 è stata tranquillamente aggirata dagli hacker, Microsoft ha confermato che alcuni hacker sono riusciti ad aggirare una delle principali protezioni antipirateria di Windows 7: l'attivazione dell'Os. Windows 7, per funzionare, richiede l'attivazione obbligatoria di entro 30 giorni dall'installazione. Questo semplice metodo, che già ci era noto con XP e Vista, è uno dei principali strumenti antipirateria che Microsoft ha messo a punto per cercare di proteggere Windows 7 da copie illegali. L'inespugnabilità è durata anche in questo caso decisamente poco... come spesso accade. Il procedimento concepito dagli hacker neutralizza efficacemente le cosiddette "Activation Technologies (Wat)" di Windows 7 poste a salvaguardia del sistema operativo. Una volta fatti i passi previsti dalla procedura, l'utente può continuare a utilizzare Windows 7 a piacimento, anche senza averlo attivato. I tecnici di Microsoft sono naturalmente già al lavoro per preparare una controffensiva. L'azienda ha anche cercato di mettere in guardia gli utenti inclini a non farsi troppi ploblemi nell'utilizzare copie illegali: spesso nelle copie pirata sono nascoste minacce per la sicurezza del sistema che sono quindi molto sconsigliate. Ciò è perfettamente vero, ma visto l'alto livello di gradimento dei prodotti Microsoft sulle reti di file sharing, sembra che la gente preferisca rischiare un possibile attacco piuttosto che spendere soldi per stare dalla parte della legalità.



DOUBLETWIST, L'ITUNES CON MENO PROBLEMI

DoubleTwist è un programma gratuito sviluppato da DVD Jon che permette di sincronizzare qualunque tipo di file multimediale con qualsiasi tipo di dispositivo portatile e ha il grande pregio di essere compatibile anche con il mondo Mac. DVD Jon è il nick name con cui l'hacker norvegese Jon Lech Johansen si fece conoscere per essere riuscito ad aggirare le protezioni dei DVD per poi concentrarsi (con successo) su altri sistemi DRM compresi quelli concepiti da Apple per iTunes. Con il graduale declino del DRM, anche l'operato del brillante norvegese ha perso un po' i diritti agli onori della ribalta, ma è comunque decisamente degno di nota. L'ultimo lavoro dell'hacker si chiama doublerTwist. Questo programma gratuito permette di sincronizzare i file multimediali fra il nostro PC e qualsiasi dispositivo compatibile con il programma. I sistemi in grado di comunicae con doubleTwist, dal funzionamento molto simile a iTunes sono tantissimi: PSP, Mac, Android, Windows, Symbian e moltissimi altri. La funzione principale di doubleTwist è quella di evitare che i DRM possano costituire un problema. Se nella nostra raccolta multimediale sono presenti file musicali, filmati o immagini con DRM, basta trascinarli nella libreria di doubleTwist: il programma si incaricherà di convertire i file nel formato adatto per essere trasferito senza problemi su qualunque dispositivo compatibile. Possiamo scaricare doubleTwist dal sito all'indirizzo www.doubletwist.com.

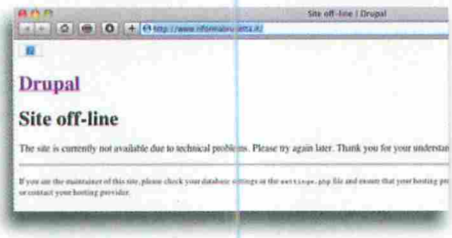




HOT NEWS

VITA DURA PER IL SITO DI BRUNETTA

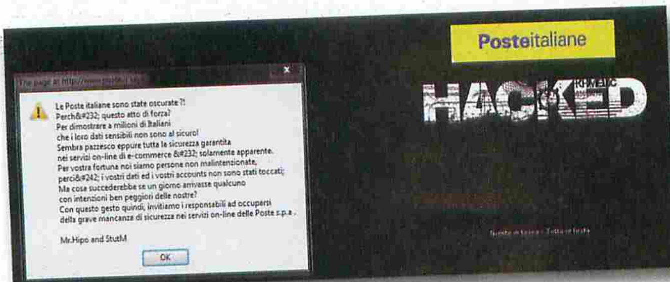
Il portale del ministero per l'Innovazione 8www.riformabrunetta.it) è stato inaugurato con un attacco di tipo DDoS (Denial Of Service) a poche ore dal lancio ufficiale. Ripristinato con sollecitudine, è caduto subito dopo. Secondo Brunetta l'azione è



stata dettata dall'ira e dall'invidia di qualche buontempone, fomentati del buon successo di circa ventimila visite al portale ad appena un'ora dal lancio ufficiale. "Tanta attenzione ha evidentemente suscitato le ire di quanti avversano l'azione del ministro per la PA e Innovazione" ha dichiarato Brunetta.

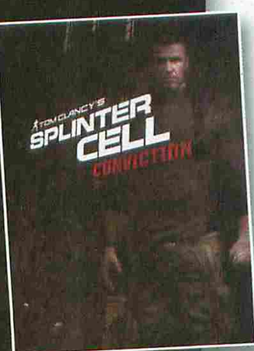
UN ALTRO ATTACCO ALLE POSTE ITALIANE

La Polizia postale e il reparto di sicurezza di Poste Italiane hanno scoperto i colpevoli dell'attacco del 10 ottobre al sito telematico delle Poste. La pagina principale del sito era stata talmente modificata che i servizi risultavano inutilizzabili dagli utenti. La polizia ha perquisito le abitazioni dei tre giovani indagati trovando abbondanti prove del reato e ha proceduto con il sequestrato di moltissimo materiale informatico, ora al vaglio dei cyber-poliziotti. L'operazione ha visto impegnati, oltre il Servizio centrale della Polizia delle Comunicazioni, anche vari compartimenti regionali della Polizia Postale. Le indagini svolte dagli investigatori del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche del Servizio polizia postale e delle comunicazioni sono state coordinate dal pool dei magistrati della Procura della Repubblica di Roma specializzati nei crimini informatici.



ATTACCO O PUBBLICITÀ

Tom Clancy's Splinter Cell è una saga che riscuote successi da anni, anche se dal 2006 non si vedono nuovi titoli per PC. Di recente, alcuni hacker hanno aggiunto dei file malevoli, dannosi per il computer, sul sito ufficiale dedicato a Splinter Cell: Conviction, il prossimo attesissimo episodio con protagonista il ben noto Sam Fisher. Per qualche tempo il sito ufficiale di Splinter Cell: Conviction, ospitato da Ubi, ha mostrato un messaggio in lingua russa e un altro breve testo che rivendica l'attacco al sito da parte di un certo Vl@d69. All'interno del codice della pagina modificata dall'hacker compariva *un collegamento* a una foto in ASCII che mostrava uno scudo con un'aquila bicefala. I maligni pensano si tratti di una mossa pubblicitaria, la versione "hackerata" del sito ha resistito un po' troppo per resistere alle possibili contromosse di un colosso come Ubi...



Sarà estradato hacker che mandò in tilt Nasa e Pentagono

L'hacker inglese Gary McKinnon verrà inesorabilmente estradato negli Stati Uniti. Il sistema giudiziario a stelle e strisce vuole metterlo sotto processo per aver violato i sistemi informatici della Nasa e del Pentagono. McKinnon venne arrestato nel lontano 2002 su richiesta delle autorità statunitensi con la pesante accusa di danni per almeno 700 mila dollari. Entrando nei sistemi americani (alla ricerca di informazioni sugli UFO, pare) dal febbraio 2001 al marzo 2002, McKinnon ha causato il blocco dei sistemi informatici della difesa *americana* proprio durante il tragico 11 settembre 2001. Come aggravante il quarantenne inglese ha anche alterato e cancellato preziosi file di una base aeronavale impegnata in operazioni critiche e ha disattivato una rete di duemila computer militari. Come spesso si legge tra le righe della nostra rivista, il difficile non è tanto violare un sistema, quanto non lasciare tracce della violazione...





Fra complex shopping narratives, realtà aumentata e hackttivismo, il lato oscuro di AppleStore

iSee

Squatting supermarkets è un'installazione interattiva che riproduce un supermercato in realtà Aumentata. Per i lettori di HJ ci siamo soffermati su iSee, il cuore tecnologico dell'installazione. iSee, applicazione iPhone basata sul riconoscimento dei loghi, usa l'infrastruttura fisica e informazionale del marketplace (punto vendita+logo) per riprogettare radicalmente atto più *estremo*, quotidiano e pervasivo del consumismo, lo shopping.

Ce lo spiega Salvatore Iaconesi, il suo ideatore, entrando nel vivo dello sviluppo e delle funzionalità del software. Alimentato da una complessa burocrazia digitale, ne emerge la descrizione del "lato oscuro" di AppleStore e delle sue politiche di accesso al codice.
Play.

HJ: "iSee" è un'applicazione iPhone: Ci spieghi meglio di che si tratta?
iSee fa essenzialmente due cose:

- trasformare i loghi dei prodotti in luoghi di comunicazione
- sovrapporre dimensioni critiche alla "realtà ordinaria

Il primo processo avviene con un sistema di riconoscimento delle immagini. Fai la foto di un logo, il software lo riconosce e ti mette a disposizione alcune possibilità:

- vedere le informazioni di responsabilità sociale ed ecologica del suo produttore
- aprire dialoghi "sul logo" (scrivere delle cose, dire delle cose, filmare

delle cose, che poi saranno consultabili dagli altri che, dopo di te, "consulteranno il logo", di fatto, trasformato in un wiki)

- creare economie ecosistemiche (se io inquadro un caffè della Nestlè, ci vedo sovraimposta la possibilità di acquistarne uno di un piccolo produttore locale, magari biologico, che non picchia i dipendenti e che adotta pratiche di sostenibilità ecologica).

Il secondo processo avviene con un semplice sistema di realtà aumentata. Geolocalizzando le informazioni si può far sì che le persone, mentre attraversano città e campagne, possano vederle direttamente sullo schermo. Ovvero, inquadri il ministero con il telefono e vedi le informazioni di una rivendicazione; inquadri un fiume e scopri che il sig. X ci ha fatto accanto una fogna non autorizzata etc...

HJ: Il progetto sembra complesso: sei arrivato a una tecnologia stabile?
Il software ed i processi ci sono. C'è solo un problema. La politica della Apple sullo sviluppo e la pubblicazione delle applicazioni sul suo AppStore. Una enorme burocrazia (fatta di contratti multipli, di certificati di firma digitale del codice, di mari di disclaimer e di condizioni e termini d'uso...) ed un processo assai complesso si affiancano ad alcune politiche "sul codice" che determinano in maniera quasi assoluta cosa può e non può essere pubblicato sullo store.
Un fatto non trascurabile perché la mancata pubblicazione sull'AppStore limita enormemente la diffusione delle applicazioni iPhone. Per prendere il software da altre parti le persone sono obbligate a sbloccare il proprio telefono. La procedura è ormai semplice, ma non alla portata di tutti e in ogni caso viola le condizioni di servizio di Apple, facendo decadere la garanzia del telefono.

HJ: Hai parlato di politica del codice. Che intendi?
Mi riferisco in particolare alle limitazioni sul software. Apple sta tenendo per sé alcune funzionalità che sono di estrema utilità per la realizzazione di applicazioni "critiche". Diversi framework presenti nell'iPhone (come la cattura di video o immagini in tempo reale, o alcune possibilità avanzate di GPS e bussola magnetica, ma anche altre più strettamente collegate alle dinamiche di interazione) sono utilizzabili solo all'interno di alcune "cornici" predisposte da Apple, con funzionalità realmente limitate. Questo avviene mantenendo private le chiamate più interessanti ed avanzate di questi sottosistemi e lasciando disponibili solo poche funzionalità in scatola.

In sintesi: i dispositivi elettronici ci sono, il software per gestirli pure, ma non li puoi usare. E se li usi (se trovi il modo di usarli) non ti permetto distribuire l'applicazione.

HJ: Sei a conoscenza di applicazioni che hanno fatto le spese di questa "politica"?
Si, in realtà c'è un ampio repertorio di casi in cui applicazioni eccellenti sono state rifiutate perché usavano i framework privati dell'iPhone. Forse il più famoso è quello di Zach Lieberman (di OpenFrameworks) che ha creato un software in grado di trasformare l'iPhone in un controller per performance audio e video. Eccezionale: coordinabile in più istanze e tra computer e dispositivi mobili, in grado di adottare protocolli standard come OSC, gratuito e OpenSource. Ma non può essere inserito nell'AppStore perché usa due librerie private, e neanche direttamente.



iSee in azione sull'iPhone.



Troviamo la presentazione iSee all'indirizzo www.toshare.it/?page_id=1074

:: Il 3° Paesaggio

Per la gioia dei lettori (e anche nostra) l'applicazione iSee sarà rilasciata con licenza Open Source ed sarà uno dei progetti editoriali curati FakePress, la neonata casa editrice cross mediale che sta già studiando il sistema in una nuova modalità dedicata alle arti performative,"re-fluxus". Intanto non ci stupiamo che Squatting Supermarkets sia stato scelto come progetto speciale di Share Festival: marketplace interstiziale che vive in squat sulle infrastrutture fisiche e immateriali esistenti proprop come un terzo paesaggio, l'operazione non si limita a detournare, irridere, svelare il market, ma lo invade riprogrammandone il codice dall'interno, costringendo a trasformare in senso ecosistemico il concetto stesso di valore.



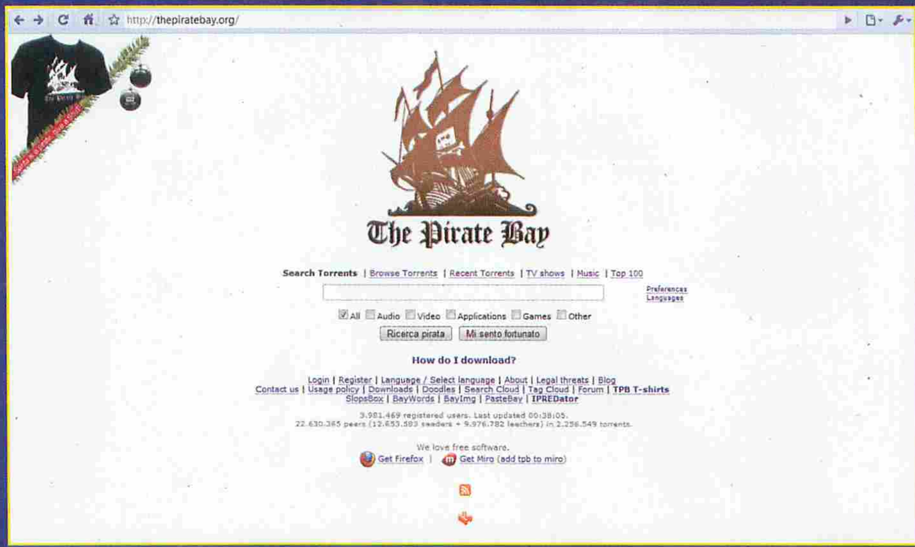
Tutti la davano morta, e in un certo senso lo è: ma The Pirate Bay si ripropone in una veste nuova è "sicura"

La Baia si rifà il trucco

La Baia è morta, viva la nuova Baia! Commento strano, ma realistico, se si pensa agli ultimi accadimenti che hanno coinvolto il servizio P2P di Peter Sunde e compagni. Senza tornare troppo su fatti che più o meno conosciamo tutti, ci basti sapere che The Pirate Bay, nella sua vecchia forma, ha smesso di esistere. Il "tracker", cioè la tecnologia che consentiva al sito di indicizzare i file, è stato infatti disattivato. Addio quindi alle nostre ricerche e relativi download assortiti? Nemmeno per sogno, tanto che una fugace visita a www.thepiratebay.org ci regala la soave vista della pagina che tanto amiamo. Il trucco, i cambiamenti principali, sono stati apportati al cuore del servizio. Dato che le accuse legali riguardavano i server che consentivano la ricerca di file torrent, i ragazzi della Baia hanno ben pensato di rinunciare proprio a questi. Il punto è che il vecchio The Pirate Bay centralizzava la ricerca dei file incriminati, e dunque poteva essere ritenuto diretto responsabile delle accuse per lesione al diritto d'autore. Ora, invece, è utilizzato il sistema dei

"magnet link". Si tratta di link che non identificano un file per il suo nome o la sua provenienza, ma per il suo "hash value". Un accorgimento che non obbliga più alla presenza di un host sempre disponibile, con enormi vantaggi sia per gli utenti sia per i gestori del servizio. Niente più client, tanto per intenderci, perché la ricerche e la gestione di The Pirate Bay avviene tutta dal browser. Con l'aiuto di due tecnologie: la Distributed Hash Table e il Peer Exchange (PEX).

La tecnologia della Distributed Hash Table (o DHT), o Tabella di Hash Distribuite, nasce intorno al 2001, per offrire una maggiore efficienza nel campo del P2P, e creare un sistema che unisca la decentralizzazione di servizi come Gnutella alla precisione di Napster (che invece era strettamente legato a un server che conteneva l'indice dei file disponibili). In effetti le DHT soddisfano proprio questi criteri, dimostrando grande velocità anche di fronte a milioni e milioni di "nodi" (cioè gli utenti). Se, dunque, la gestione dei nodi di The Pirate Bay è affidata a questa entusiasmante Distributed Hash Table, resta da vedere cosa succede quando si scende a livello di nodo. Insomma, che rapporto c'è tra nodo e nodo? Come comunicano tra loro? Con la seconda tecnologia che abbiamo nominato poco fa: la PEX, o Peer Exchange. In pratica, nella classica architettura di BitTorrent, il gruppo di utenti che collaborano per mettere in condivisione un file è detto "swarm". Lo swarm è intimamente legato a un tracker, che di fatto ha la responsabilità di mettere in contatto tra loro i diversi utenti. Il Peer Exchange, invece, mette in contatto diretto i componenti dello swarm, non basandosi dunque sul tracker. Uno dei metodi più efficaci per crare e gestire un PEX è generare una DHT, e qui il cerchio si chiude: DHT e PEX sono la "coppia perfetta" pronta a garantire lunga vita ed efficienza al nuovo The Pirate Bay.



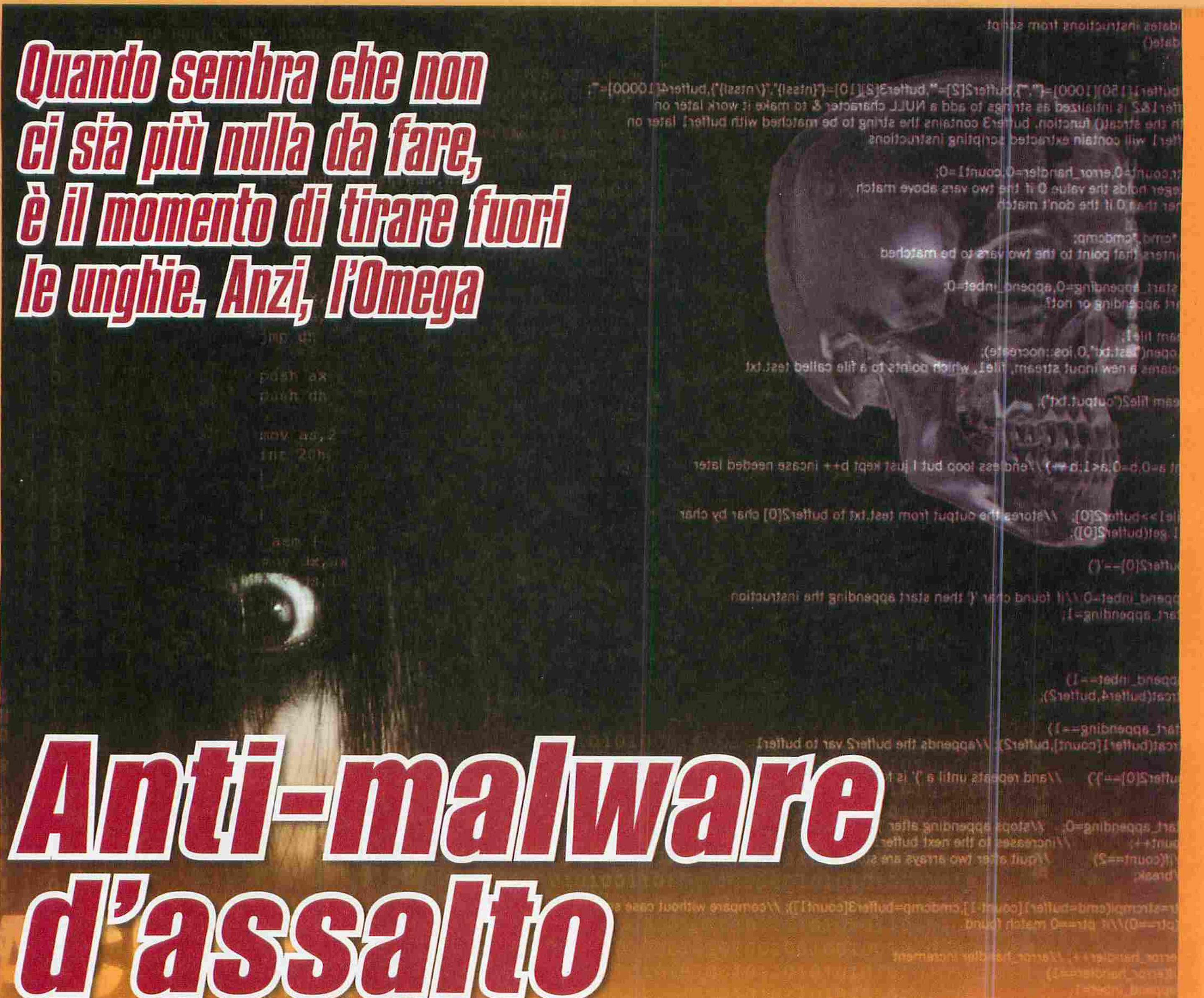
Il nuovo look della Baia è minimalista e richiama vagamente quello di Google.

Il connubio di tutte queste tecnologie, dunque, è un cuore nuovo per la Baia dei Pirati, che offre innumerevoli vantaggi e pochi passi indietro. Tra questi ultimi, una precisione nei risultati di ricerca al momento leggermente inferiore. I sistemi totalmente indicizzati se la cavano meglio, sotto questo punto di vista, ma è pur vero che le DHT consentono di programmare funzioni in grado di direzionare al meglio le stringhe inserite dagli utenti. E pare che gli sviluppatori stiano già lavorando in tal senso...

Tanti invece, come detto, i vantaggi del nuovo corso di The Pirate Bay. La sicurezza per la privacy degli utenti, innanzitutto, visto che DHT e PEX consentono di raggiungere una totale decentralizzazione dei contenuti. Senza parlare, di nuovo, della sicurezza per chi il servizio lo gestisce: le Autorità cercheranno nuovi cavilli a cui appigliarsi, certo, ma siamo abbastanza sicuri che, questa volta, i ragazzi della Baia sentiranno meno fiato sul collo di quanto accaduto in passato.



Tra le opzioni di download dei Torrent fa bella mostra di sé il magnet link.



Quando sembra che non ci sia più nulla da fare, è il momento di tirare fuori le unghie. Anzi, l'Omega

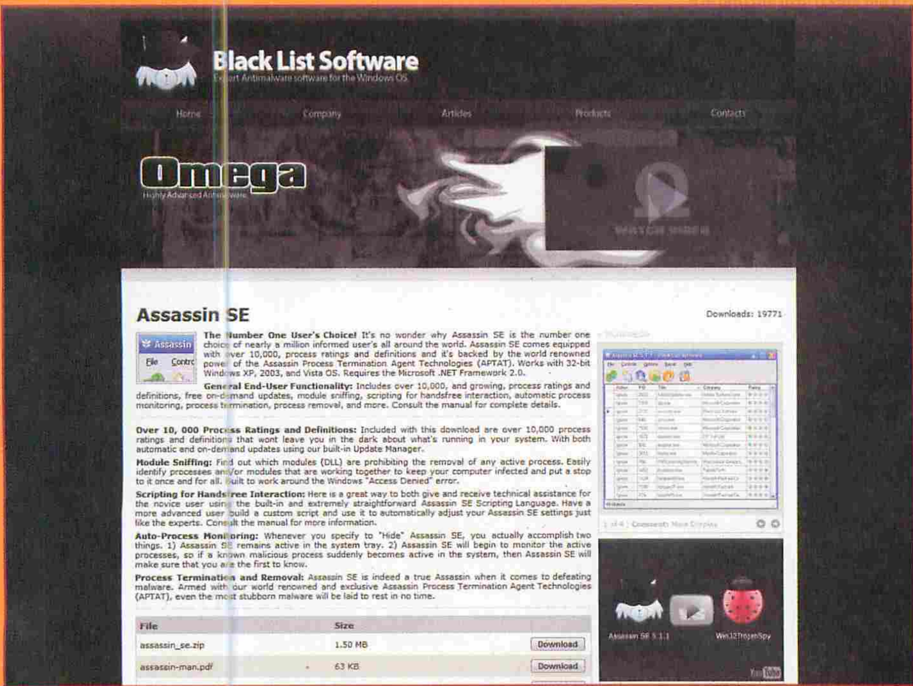
Anti-malware d'assalto

Gli attacchi cracker hanno molteplici scopi e obiettivi, ma, scava scava, ben poche modalità. Una di queste è la penetrazione nel sistema avversario e l'immissione di malware di vario tipo. Trojan, worm, codice sviluppato ad hoc per mettere al tappeto il sistema della vittima di turno. Quando ciò succede, infatti, il computer avversario passa sotto il controllo dei software malevoli, che ne rallentano, o bloccano, i processi vitali. In queste situazioni il classico antivirus è un palliativo blando come non mai, incapace di fermare efficacemente l'avanzata dei byte nemici. Black List Software, azienda specializzata nello sviluppo di software per la rimozione dei malware, ha da poco rilasciato Omega CE, programma potentissimo che consente di eliminare il codice nocivo senza bisogno di avviare il sistema operativo del computer-vittima. Come? Con un trucco vecchio (quasi) quanto i computer: si appoggia a un piccolo kernel da caricare nella fase di boot del computer, passando poi il controllo a Omega CE.



:: Disponibile fin da subito

Omega CE è scaricabile gratuitamente, in versione beta, dalla pagina blacklistsoft.com/omega.php. Una volta qui, basta un clic sul rispettivo



Black List Software, in precedenza, è assorta agli onori della cronaca per Assassin SE, software per il controllo dei processi di sistema.

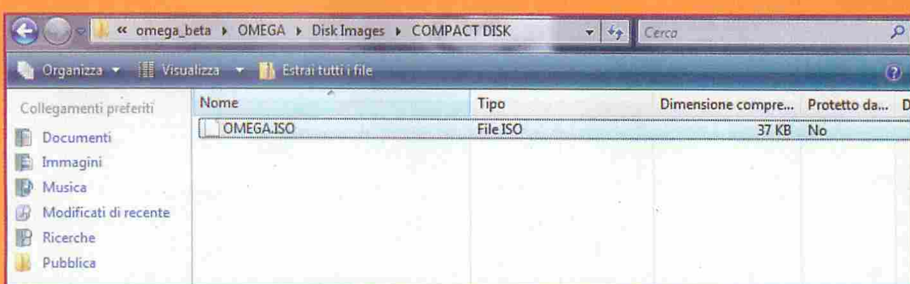
Download per scaricare il file omega_beta.zip. Un archivio ZIP di, sorpresa, appena 96 Kb. Al suo interno troviamo la cartella Omega, e la sottocartella Disk Images. Considerando che il file include anche un PDF da 39 Kb, si rimane sconvolti da cosa si può ottenere con del codice ben organizzato e implementato. Alla faccia delle centinaia di megabyte necessari a un qualunque antivirus o, peggio ancora, dei gigabyte di alcuni sistemi operativi... Come detto, il file di Omega CE propone delle "immagini": una per il boot da floppy disk (sottocartella FLOPPY DISK) e una per quello da CD (sottocartella COMPACT DISK). La prima è in formato IMA, mentre la seconda nel classico ISO. Nella maggior parte dei casi, com'è ovvio, si utilizza la seconda, masterizzando un CD o DVD con un software apposito. Se non ne abbiamo uno a portata di mano, una soluzione veloce ed efficiente è PCWin ISO Burn, disponibile gratuitamente su www.frontierdg.com.

:: Un riavvio e Mega CE si... avvia

Effettuata la masterizzazione, basta inserire il disco nel lettore e riavviar e il computer, di modo che effettui il boot col kernel di Omega CE. Dopo qualche istante, il software è già all'opera, con un primo controllo del disco. A questo punto, giunti nella scarna finestra principale (e non poteva essere altrimenti, viste le esigue dimensioni del file di partenza), non resta che far partire il controllo. Il punto di forza di Omega CE, innanzitutto, è che col suo approccio è in grado di accedere a un sistema Windows anche quando questo è talmente compromesso da non potersi nemmeno avviare. E meno male: la mancanza di boot del sistema operativo principale non dà modo ai malware di "legarsi" ai processi in esecuzione, agevolando al loro eventuale rimozione. Una volta davanti alla finestra di Omega CE, è sufficiente inserire il nome dell'oggetto da ricercare e attendere che sia rilevato. Il sistema di Black List Software, infatti, non si basa su database predefiniti (ciò comporterebbe la necessità di un continuo aggiornamento), ma richiede per lo meno che si conosca il nome dei file infetti, o infettanti. A questo punto, si ha modo di eliminarli o "bloccarli", isolandoli dal resto del sistema. Riavviando il computer e tornando in Windows, i file rimangono bloccati, dandoci modo di studiarli o verificare che *siano effettivamente* questi l'origine dei nostri problemi.

:: Strumento per esperti

Per semplicità dell'interfaccia e (leggera, suvvia) difficoltà d'utilizzo, Omega CE è ovviamente rivolto a utenti esperti. Non è un antivirus, ma proprio un antimalware in senso stretto: uno strumento, cioè, in grado di isolare ed eliminare il codice malevolo. La sua efficacia, del resto, dipende dal grado di competenza di chi lo utilizza.
Al momento, Omega CE, come detto, è in una versione " 2.0 beta", che si distacca nettamente, per efficienza, velocità e potenza da quella originaria. Tuttavia Black List Software ha ancora del lavoro da sistemare, visto che, dalle nostre prove, è emerso qualche bug che inficia l'operatività dell'interfaccia. I trackpad di molti netbook e notebook, per esempio, non funzionano o funzionano male, rendendo piuttosto difficoltoso l'utilizzo del programma. Niente, comunque, che non possa essere risolto. La tecnologia centrale, quella antimalware, del resto, funziona benissimo. Per i fronzoli c'è tempo.



In questo piccolo file-immagine, di appena 37 Kb, troviamo tutto il necessario per creare il disco d'avvio di Omega CE masterizzandolo su un CDvergine



A RISCHIO CYBERGUERRA

Una rete di computer, hacker preparati e la ricetta è servita: la guerra via web è più reale di quanto pensiamo

In principio ci fu Titan Rain, definizione data a quella serie di attacchi che, a partire dal 2003, colpirono gli Stati Uniti. Non attacchi militari in senso stretto: attacchi via rete, sfruttando le linee telematiche e mettendo KO numerosi computer, tra i quali quella della Lockheed Martin e della NASA. Poi, nel 2007, fu la volta della Estonian Cyberwar. Altra guerra telematica, ma più raffinata: a partire dal 27 Aprile 2007, e per numerosi giorni, un serie coordinata di attacchi di tipo Denial of Service colpì siti governativi, e non, dell'Estonia. Con Titan Rain la colpa fu addossata (ovviamente) ai cinesi, mentre nell'Est europeo si puntò il dito contro (ri-ovviamente) i russi. Evidenze di queste responsabilità, però, non ce n'erano, tanto che il clima tra

i paesi coinvolti andò rapidamente a surriscaldarsi. Insomma, un attacco telematico rischiava di tramutarsi in un formale attacco militare. Perché il rischio delle guerre telematiche, o cyberwar, è esattamente questo: creare pretesti per operazioni militari magari pianificate da tempo. Queste poche righe descrivono una certa facilità nel portare un conflitto dallo schermo di un computer a un teatro di guerra (ahinoi) in carne ed ossa. E le cose, in effetti, stanno effettivamente cosi'. La speranza, dunque, sarebbe quella di rendere altamente improbabili le cyberwar, ma la doccia fredda arriva anche da questo versante. Si tratta di una possibilità tutt'altro che remota e se leggiamo da un po' questa rivista non ci è difficile capire il perché: effettuare un attacco hacker ai danni di un server non è in fondo difficile, se si ha padronanza della materia, e quando le cose si fanno complesse gli hacker tendono a lavorare in gruppo e scavalcare qualsiasi tipo di difesa.

::Dall'origine all'impatto

Al momento la gravità di un cyberattacco è valutata secondo quattro distinti parametri: origine, motivazione, sofisticatezza e impatto; e stando a un recentissimo rapporto di McAfee, nessuno degli attacchi fin qui perpetrati ha superato la soglia di pericolosità. Quella, insomma, che fa passare per davvero un cyberattacco allo stato di cyberguerra (cyberwar). Anche il recente attacco a Stati Uniti e Korea del Sud, benché preoccupante, non è classificabile come cyberwar, ma per modalità e intensità lascia supporre che non manca molto a uno scenario di web-soldati pronti a interferire nelle linee (telematiche) nemiche. Quanto accaduto nel Luglio 2009, infatti, ha dei risvolti più politici che economici, e questo è visto dagli esperti come una chiara avvisaglia che l'attacco hacking si è trasformato in un atto di forza contro Stati Uniti e Korea del Sud. Ovvio che sul banco degli imputati è stata prontamente messa la Corea del Nord. Stando a una dichiarazione della Seoul's National Intelligence Service (NIS) "non è [stato] un semplice attacco di singoli". Certo, è pur vero che gli attacchi di gruppo non sono certo nuovi nel mondo della sicurezza informatica, ma la NIS è certa dell'origine nordcoreana, e quindi politica, di questo.

Le capacità informatiche della Corea del Nord sono note, anche se, stando a un recente rapporto di McAfee, sono altri i paesi in prima linea nel campo della cyberwar. I "magnifici cinque" sono Cina, Stati Uniti, Russia, Francia e Israele. Pare che queste nazioni, da qualche anno, stiano ingaggiando i migliori hacker del mondo, dotandoli di strumenti software in grado di penetrare nei sistemi avversari.



Il controllo dei sistemi bellici, anche quelli di distruzione di massa, è affidato ad elaboratori. E spesso questi fanno parte di reti...

::Il rischio c'è

Siamo dunque alle soglie della guerra telematica? L'attacco di Luglio fa supporre di sì, perché ha fatto da varo a un nuovo tipo di Denial of Service. Sofisticato, difficilmente tracciabile e, soprattutto, veloce. Talmente veloce da aver diffuso un malware in reti da migliaia di computer, in pochi istanti, congestionando il loro traffico e mettendole al tappeto. Insomma: è chiaro che lo si potrebbe considerare un collaudo per abbattere le difese della fazione nemica, e quindi mettere a segno i propri colpi.

Stando a Bkis Security, l'origine nordcoreana dell'attacco non è certa: per perpetrarlo è stata utilizzata una botnet di ben 166098 computer sparsi per tutto il globo, ma comandati da otto server che facevano capo a uno localizzato nel Regno Unito. Curiosità: utilizzava Windows Server 2003 come sistema operativo.

Resta il fatto che la preoccupazione è salita alle stelle, anche in casa del Presidente Obama. Il quale, dopo aver istituito, nel Maggio scorso (quindi prima dell'attacco), un'agenzia di cyber-security, ha concordato col Pentagono un sostanzioso potenziamento della struttura. Anche la Corea del Sud cerca di attrezzarsi, visto che il suo dipartimento Defence Security Command ha rilevato circa 95000 tentativi di accesso alle sue reti militari, in appena un mese.

Risalire agli autori è tutt'altro che facile, al punto che gli sforzi sembrano più orientati a creare delle difese migliori contro i prossimi attacchi. La progressiva connessione in rete di sistemi militari di alto livello, getta ulteriore benzina su uno scenario già infuocato: elaboratori spesso isolati da qualsiasi rete, perché contenenti informazioni e software dalla potenza bellica devastante, rischiano di cadere sotto il controllo del nemico in caso di attacco telematico. E a quel punto la cyberwar diventerebbe reale quanto una testata nucleare a lungo raggio...



SKY Card Sharing

Come aggirare le protezioni delle codifiche satellitari e condividere gli abbonamenti

Questo articolo non contiene informazioni volte a stimolare l'uso improprio di un regolare abbonamento dei provider satellitari, ma presuppone che il pubblico cui è diretto sia interessato a capire meglio come funziona il processo di decodifica di un canale criptato.

:: Un po' di storia

Qualche anno fa la pirateria satellitare in Italia raggiunse il suo apice nel momento in cui venne bucato il sistema di codifica SECA utilizzato al tempo da TelePiù e Stream. In rete si potevano trovare ovunque guide e tutorial legati al come vedere "a scrocco" i canali satellitari a pagamento e fiorì un commercio al limite della legalità di strumentazioni elettroniche volte a simulare o alterare abbonamenti reali (questa chiaramente una pratica illegale). Una stretta minoranza di persone studiava invece le codifiche adottate al solo scopo di conoscere le tecnologie messe in campo e a mio modesto parere erano quelli che si divertivano di più, soprattutto quando assistevano agli "attacchi dei provider" e alle relative contromosse dei pirati.

A fine 2002 il gruppo News Corp. di Rupert Murdoch, già proprietario di Stream, rilevò Telepiù per creare SKY Italia, piattaforma unica satellitare che fino a pochi mesi fa costituiva il monopolista del settore in Italia (di recente infatti con la partenza di TivùSat sta arrivando un po' di concorrenza che certamente farà bene ai consumatori). Con la partenza della nuova piattaforma venne adottata la co-



Tra i prodotti che rendono possibile questa operazione ricordiamo Dreambox, il top dei decoder sat.

difica NDS, sempre di proprietà di News Corp., che risulta tuttora inaffondata e che apparentemente ha chiuso giochi (e gli affari) di quanti si erano industriati in tal senso fino allora.

:: Card-Sharing

Apparentemente, perché già qualche tempo fa, si era sparsa la notizia che interi condomini riuscivano a condividere un unico abbonamento tra i vari appartamenti, grazie a un server centrale che ripeteva il segnale. SKY offre ora qualcosa di simile ma a pagamento.

Di recente però c'è stata una notevole evoluzione che permette di vedere i canali di SKY se non gratis, sicuramente a un prezzo decisamente inferiore a quello di listino: il Card-Sharing.
Supponendo di avere un decoder satellitare riprogrammabile, in cui viene alloggiata una smart-card cui è associato un regolare abbonamento (mettiamo per esempio il pacchetto Cinema), collegato via Internet a un altro decoder in cui è alloggiata un'altra smart-card cui è associato un diverso regolare abbonamento (con ad esempio il pacchetto Calcio), grazie a un software di condivisione delle chiavi, i due decoder sono in grado di mettere in chiaro le trasmissioni criptate di entrambi i pacchetti, perché nel momento in cui viene richiesto di decodificare un canale per il quale il decoder non ha i diritti di visione, la richiesta verrà instradata verso la carta alloggiata nel secondo decoder.
Una struttura del genere è possibile perché pur non violando l'algoritmo alla base della codifica adottata, è possibile intervenire nel processo di decodifica che si realizza tra la CAM (Conditional Access Module, il modulo di accesso condizionato che fa parte del decoder) che gestisce il flusso dei dati cifrati e la smartcard che contiene i diritti di visione. Se la richiesta proviene infatti da una CAM locale o remota, poco importa: la smartcard svolgerà il suo compito e darà "luce" al canale del quale sta ricevendo la trasmissione criptata. Per gestire una struttura client/server si può scegliere di attrezzare un pc per farlo diventare una stazione di decodifica (andrà quindi inserita una scheda di decodifica satellitare e un lettore esterno di smart-card chiamato Phoenix o SmartMouse) su cui installare tutto il software, oppure utilizzare uno dei decoder evoluti basati su Linux che permettono di essere continuamente aggiornati lato firmware o lato software, con i vari plugin che vengono rilasciati quotidianamente. Il più famoso di questi decoder si chiama Dreambox.

NoeXKuzE



Il Phoenix (o smartmouse) è lo strumento ideale per comunicare con una una smart-card, ma diventa inutile se non si sa nulla della codifica utilizzata

CONDIVIDERE UN ABBONAMENTO

Supponiamo di avere due Dreambox in due stanze diverse e un solo abbonamento. Colleghiamo i due Dreambox tramite la porta ethernet con un cavo cross, oppure tramite un hub o switch e due cavetti di rete. Lanciamo su entrambi "setup-expert setup-network settings" e inseriamo gli indirizzi di rete; ad esempio:

- **Dreambox #1**
  IP 192.168.0.1
  subnet 255.255.255.0

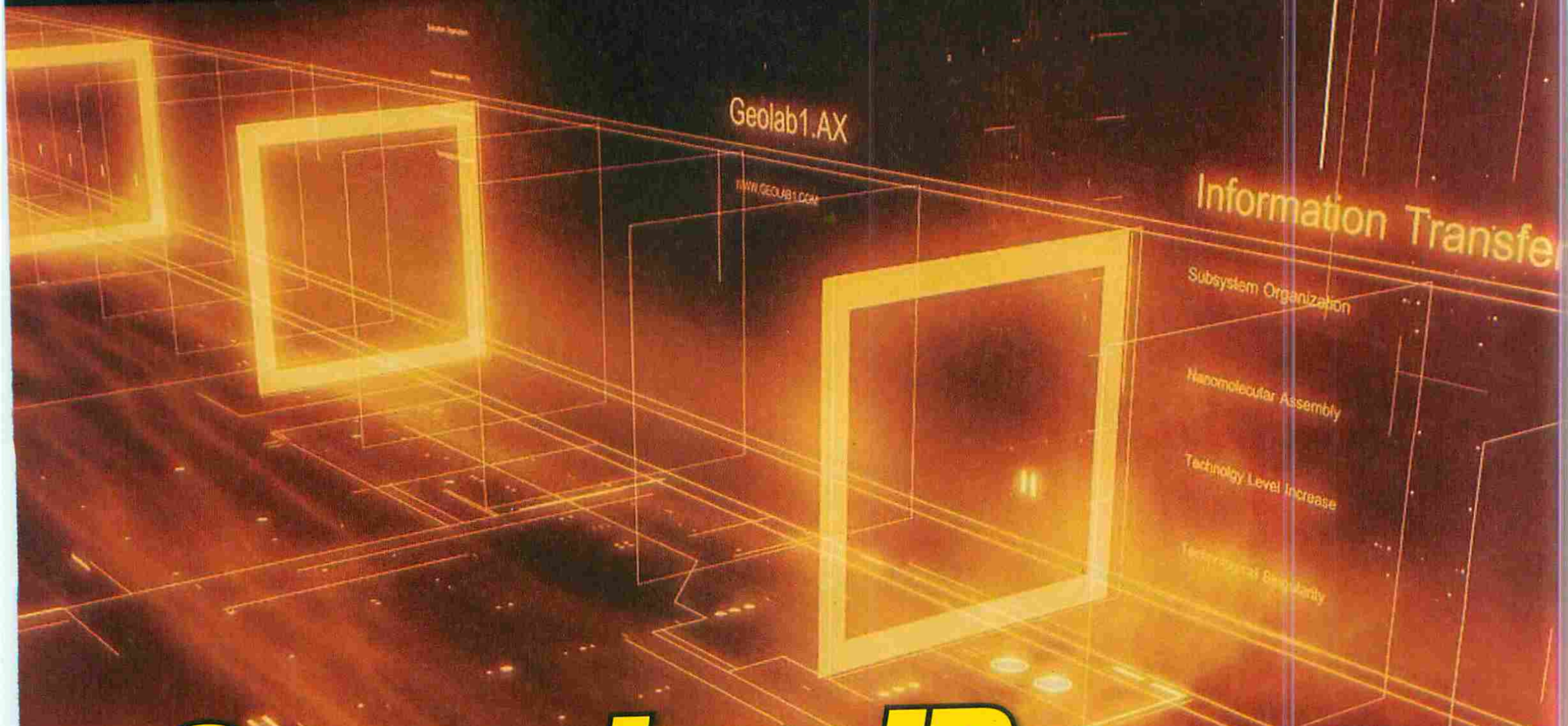
- **Dreambox #2**
  IP 192.168.0.2
  subnet 255.255.255.0.

Ora dobbiamo installare il server per il Card-Sharing e ne esistono diversi. Il più famoso è NewCS (il server) cui si connette Newcamd (il client). Dopo averlo rintracciato in rete e installato, possiamo configurarlo tramite il file Newcs.xml (/var/tuxbox/config). Nella sezione **<debug>** inseriamo **<udp_host>192.168.0.1</udp_host>**, nel decoder che fungerà da server. Poi cerchiamo **<udp_port>10000</udp_port>** e inseriamo la porta che vogliamo dedicare al server. Nella sezione **<newcamdserver>** indichiamo il nome del server: **<name>testserver</name>**. Poi inseriamo **<deskey>01 02 03 04 05 06 07 08 09 10 11 12 13 14</deskey>**, che rappresenta il codice di accesso per gli utenti. Più avanti impostiamo nome utente e password nella sezione **<user>**.

La configurazione server/client viene stabilita in Newcamd.conf (/var/tuxbox/config/newcamd). Qui dobbiamo trovare la riga che imposta il CWS con questa struttura:

CWS = 192.168.0.1 10000 username userpass 01 02 03 04 05 06 07 08 09 10 11 12 13 14 lan test server

Sostituendo a username e userpass i dati che abbiamo inserito in Newcs.xml.
L'ultimo passo riguarda l'emulazione della CAM che interviene nel momento in cui la richiesta deve essere inoltrata alla CAM fisica dell'altro decoder. Occorre installare CCcam e inserire il codice di accesso già inserito in precedenza anche nel file CCcam.cfg (/var/etc/). Completate le modifiche entrambi i Dreambox vanno riavviati e saranno pronti a gestire il card-sharing dell'abbonamento scegliendo da menu "CCcam + Newcs" (o simile).



Scanning IP rapido e indolore

Con Advanced IP Scanner 1.5 controllare lo "status" degli indirizzi IP è questione di secondi!

A molti l'utilizzo di un IP Scanner sembra inutile, o ridondante, ignorando che questo è uno degli strumenti principi quando si parla di "footprinting". A chi di noi all'ascolto non sa di cosa si tratta, diciamo che il footprinting, in buona sostanza, è il primo passo di qualsiasi azione hacker. Mica male, vero? Bene, scopo del footprinting è la raccolta di tutte le informazioni possibili e immaginabili sul computer e/o la rete che costituisce l'obiettivo delle nostre azioni. Capiamo bene che le "informazioni" sono davvero tante, e spaziano dalla scelta degli indirizzi IP alle caratteristiche intrinseche di una rete, passando per blocchi, tipi di router e via dicendo. Ed è proprio nel footprinting, come detto, che un IP Scanner dimostra la sua massima utilità, perché consente di stabilire se un dato indirizzo IP offre o meno una "risposta". In caso affermativo, significa che quel dato IP esiste e, dunque, è "operabile".

:: Per un attacco più preciso

Un momento: cosa significa che un indirizzo IP fornisce una risposta? In soldoni, che inviandogli delle richieste di dati ne otteniamo in risposta, e questo è un chiaro segnale che quell'indirizzo IP è vivo e vegeto. Gli indirizzi IP, come sappiamo, sono milioni e milioni, molti dei quali scelti e allocati al momento. Quindi non è

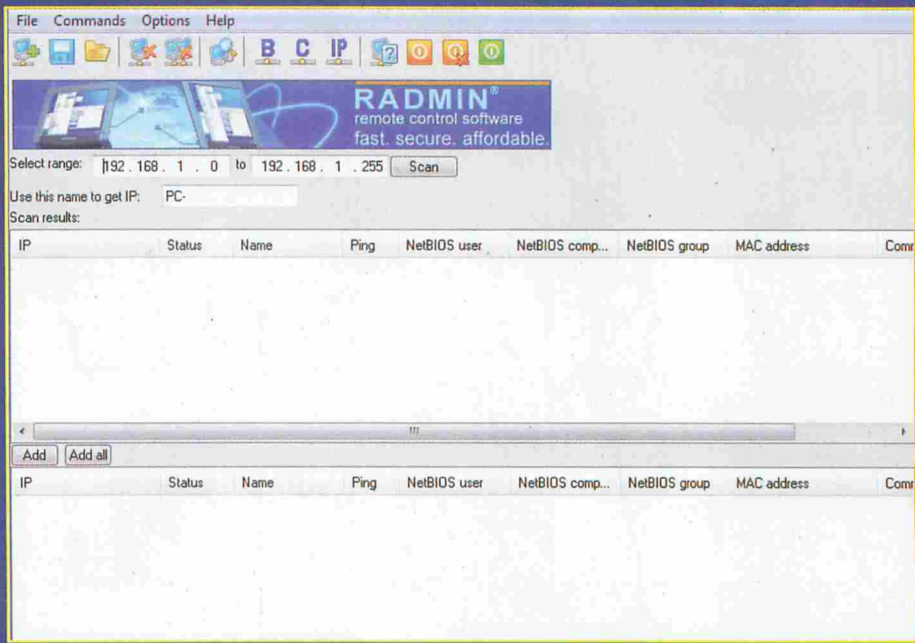
detto che un indirizzo IP sia utilizzato. Scagliarsi a testa bassa contro svariati IP, senza tenere conto del loro stato, è un metodo stupido di agire, perché rischiamo di operare su indirizzi inutilizzati, sprecando risorse e tempo. Molto meglio, quindi, utilizzare un IP Scanner, per vedere se un IP è attivo o meno. Advanced Ip Scanner è uno dei migliori software di questa categoria, per via di una velocità da record e una buona semplicità d'utilizzo: possiamo dargli in pasto grandi intervalli di indirizzi IP, e in pochi secondi otteniamo lo stato operativo di tutti. Una manna, quando si tratta di direzionare in modo preciso controlli, attacchi e via dicendo.

:: Scarichiamolo gratuitamente

Troviamo Advanced IP Scanner (o AIPS), nella nuova e scintillante versione 1.5, nella pagina ufficiale www.radmin.it/products/utilities.php. Compatibile con Windows, a partire dalla versione 95 in poi, sia per sistemi a 32 che 64 bit, AIPS nasce per il controllo degli IP di reti locali, spesso il principale bersaglio di attacchi informatici. Per scaricarlo, dalla pagina clicchiamo sulla rispettiva voce Scarica. Quindi, facciamo doppio clic sul file ipscan15.exe, clicchiamo su Esegui e su Consenti, ed eccoci nella finestra d'installazione. Spuntiamo la casella I agree with the above terms and conditions, poi clicchiamo su Next e su Start. Dopo un istante, il programma è installato nel nostro computer, e per avviarlo non ci resta che selezionare Start/Tutti i programmi/Advanced IP Scanner/Advanced IP Scanner.

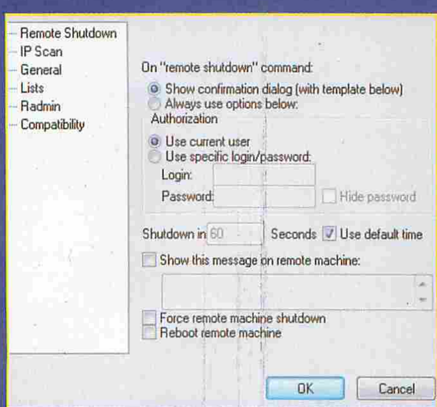
:: Facile, veloce e potente

Se non abbiamo mai utilizzato un IP Scanner, l'interfaccia principale di AIPS ci sembrerà un tantino scarna, in caso contrario ne gioiremo, abituati come siamo a software da usare a riga di comando. L'uso di Advanced IP Scanner è elementare: in Select range specifichiamo



È vero, l'interfaccia appare scarna, del resto i dati da immettere sono solamente due: IP di partenza e IP finale, al resto dobbiamo pensare noi.

un intervallo di indirizzi IP (quello di partenza e quello finale), quindi non ci resta che cliccare su Scan. Fine della storia, davvero: la scansione ha inizio e il tempo di attesa varia a seconda dell'ampiezza dell'intervallo impostato, e naturalmente della velocità della nostra connessione. Il rapporto finale elenca, in modo chiaro e comprensibile, gli indirizzi IP dell'intervallo presi in esame, rivelando per ciascuno lo Status, Name, Ping, NetBIOS user, NetBIOS computer, NetBIOS group e MAC address. L'informazione



Tante le opzioni a disposizione. Alcune, tra l'altro, consentono di attivare delle funzioni molto avanzate.

essenziale è, ovviamente, lo Status: se questo è alive possiamo operare agevolmente su di esso. In caso contrario, non è detto che l'indirizzo IP sia inutilizzato, magari c'è un firewall che attua un hiding del medesimo, tuttavia gli esiti di eventuali azioni non sono garantiti. Come anticipato, Advanced IP Scannner nasce per il controllo di reti locali (LAN), ed è su questo versante che offre alcuni sfiziosi comandi. Per esempio il Wake-On-Lan remoto, o la possibilità di collegarsi a un computer sfruttando il protocollo FTP anziché quello HTTP. Se poi crediamo che il controllo di reti locali sia meno interessante o utile rispetto a quello di indirizzi esterni, forse è il caso di pensare alla rete dell'azienda o a quella di istituto o università dove lavoriamo: gli spunti non mancano davvero...
Come nota finale, Advanced IP Scanner è un complemento ideale a Radmin 3.4 Remote Control Software, programma di controllo remoto, a pagamento (ma nel sito è disponibile anche una versione gratuita valida per 30 giorni), realizzato dalla medesima software house. Una bella coppia per davvero, specie quando si tratta di prendere il comando di un terminale altrui.

Disponibile la nuova versione di uno dei più efficienti software crittografici: ecco tutti i suoi segreti

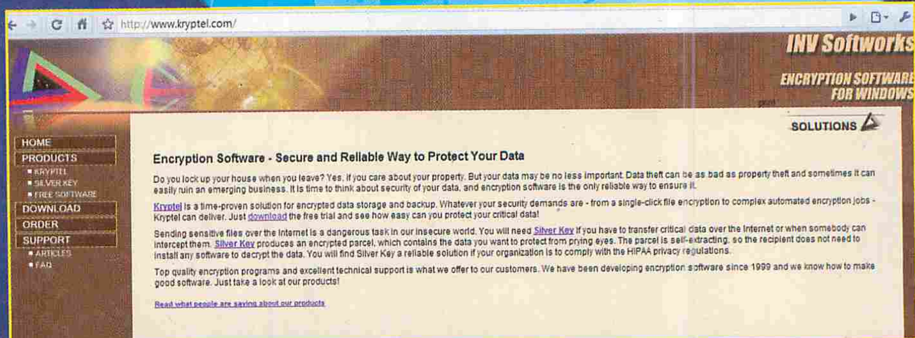
Crittografia facile e potente



Non esistono i software "tutto in uno". O meglio: esistono, ma spesso e volentieri funzionano male. Nel campo della sicurezza informatica questo, se possibile, è ancora più vero. Meglio puntare a software che eseguano una sola funzione, ma lo facciano bene. Ecco spiegato l'alone di diffidenza che circonda anche i programmi dedicati alla crittografia: ce ne sono molti che si vantano di supportare tutte le tecnologie di codifica dei dati, di farlo in modo veloce, di farlo in modo efficiente, e via dicendo. Ma la verità è che, fino a questo momento, nessuno è riuscito a ripagare attese e speranze. Già, fino a questo momento.

:: Una versione matura

Partito un po' in sordina, infatti, Kryptel ha raggiunto la versione 5.92, e promette di soddisfare le esigenze di chi ha bisogno di uno strumento di crittografia veloce, ideale per proteggere dati con grande frequenza, e chi invece della sicurezza dei propri dati fa tesoro o professione. E quindi necessita di algoritmi complessi. Qualunque sia la nostra esigenza, questo Kryptel permette di



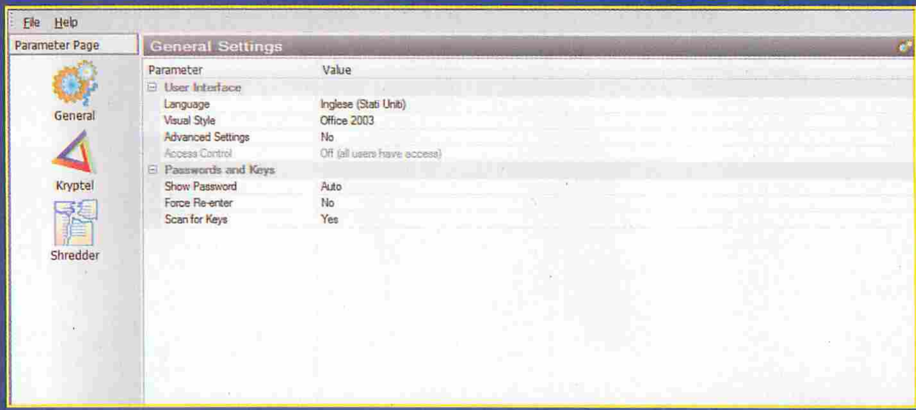
▲ Il sito ufficiale di Kryptel mette a disposizione anche Silver Key, software maggiormente orientato allo scambio via Internet di dati criptati.

gestirla tramite un'interfaccia gradevole, che permette di agire su cartelle e file.

:: Dal download all'uso

Il nuovo Kryptel è disponibile per tutte le versioni di Windows, dalla 95 in poi, con una licenza di tipo shareware. Ergo, abbiamo ben trenta giorni per sperimentare e capire se le nostre necessità valgono una spesa di 29,95 $. E la risposta, quasi sempre, sarà "sì". Andiamo quindi sul sito www.kryptel.com, clicchiamo a sinistra, su Download, e poi di nuovo su Download per scaricare l'ultima versione del software. Facciamo quindi doppio clic sul file eseguibile e clicchiamo su Esegui e Consenti. Una volta avviata la procedura d'installazione, nella prima finestra clicchiamo su Next, spuntiamo la casella Yes, I agree with all the terms of this license agreement, e clicchiamo su Next fino a che l'installazione ha inizio. Alcuni firewall possono chiederci il permesso di copiare i file del software: acconsentiamo. Al termine dell'installazione, clicchiamo su Finish. Kryptel, a questo punto, è installato e funzionante nel nostro computer, e a confermarlo c'è la rispettiva icona nell'angolo in basso a destra del desktop (se non compare, può essere necessario un riavvio del computer). Adesso non ci resta che aprire un'unità disco fisso o una cartella, e stabilire quale file (o cartella) codificare. Basta farci sopra un clic col tasto destro e selezionare il comando Encrypt. Compare la finestra Enter Password:, dove specificare la password desiderata. Qui Kryptel sfoggia un'opzione di alto livello, vale a dire la tastiera virtuale richiamabile con un clic su Keyboard. Non è banale, perché consente di scavalcare l'uso di tastiere fisiche e, quindi, evitare di essere spiati da eventuali keylogger (i "clic", infatti, non sono intercettabili da questi software). Inserita la password, clicchiamo su Ok e, in pochi istanti, il file o la cartella sono crittografati come richiesto. Tentare di aprire il file generato, a questo punto, visualizza una finestra ove inserire la password stabilita. Se è corretta, accediamo al Kryptel Browser, con cui gestire il contenuto del file criptato senza bisogno di decodificarlo. Certo, è comunque possibile farlo da qui, ma la prassi più rapida è di clicca col tasto destro sul file criptato e selezionare Decrypt. Di base, il funzionamento del programma sta tutto qui, davvero. Una manna anche per chi sa poco o nulla di crittografia, ma vuole proteggere in modo sicuro i propri dati: Kryptel, infatti, permette l'utilizzo di password lunghe fino a 4096 caratteri (!!!). Gli algoritmi utilizzati sono di quelli da far venire gli occhi lucidi a esperti e maniaci di sicurezza: AES (Rijndael), triplo DES, Blowfish, Twofish, Serpent e IDEA. Insomma, dietro un'interfaccia così semplice, in realtà, batte un cuore tecnologico di prim'ordine.





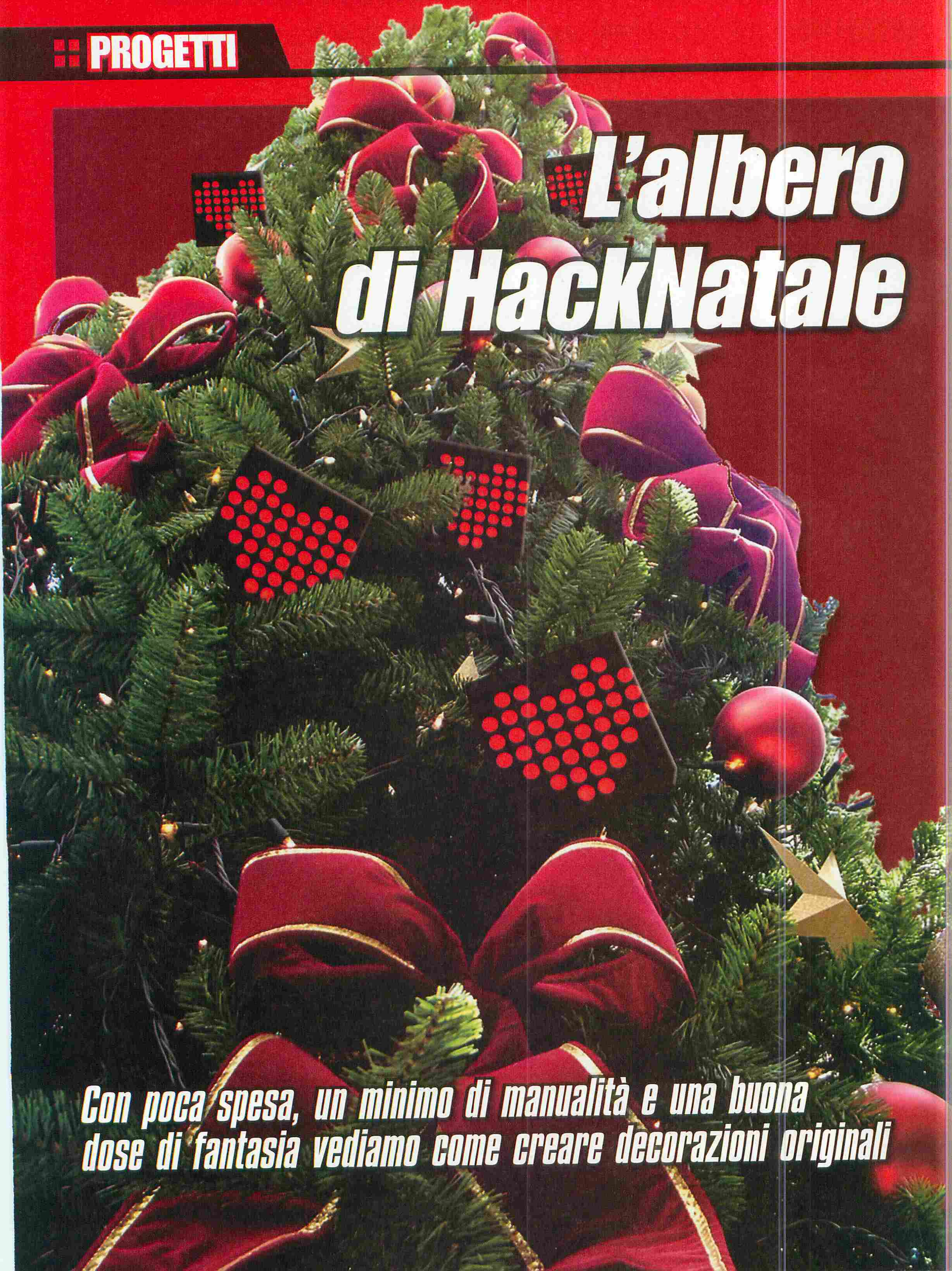
Ogni parametro di Kryptel è configurabile, grazie all'apposita sezione Crypto Settings.

:: Anche chiavi binarie

Ad avallare l'impressione di un software dedicato anche ai professionisti, la possibilità di utilizzare chiavi anziché password. La differenza appare sottile, ma è sostanziale: una chive, infatti, è un numero binario lunghissimo, da memorizzare in un dispositivo portatile che, a questo punto, può essere utilizzato come "chiave elettronica". Così, quando è necessario decodificare un file criptato, è sufficiente inserire il dispositivo (dischetto, CD, DVD, memoria USB e via dicendo) e richiamare la chiave in formato KF. Per creare una chiave binaria è sufficiente avviare il menu Start/Tutti i programmi/Kryptel/Advacend Tools, e selezionare Create Binary Key. Nella finestra visualizzata, inseriamo un testo assolutamente casuale, di lunghezza compresa tra i 100 e i 200 caratteri, e clicchiamo su Ok. A questo punto compare la finestra Key Creation, dove specificare il dispositivo ove memorizzare la chiave. Eventualmente, possiamo specificare il disco fisso e copiarla nel dispositivo in un momento successivo, ma ricordiamoci che il nostro computer potrebbe essere "spiato".

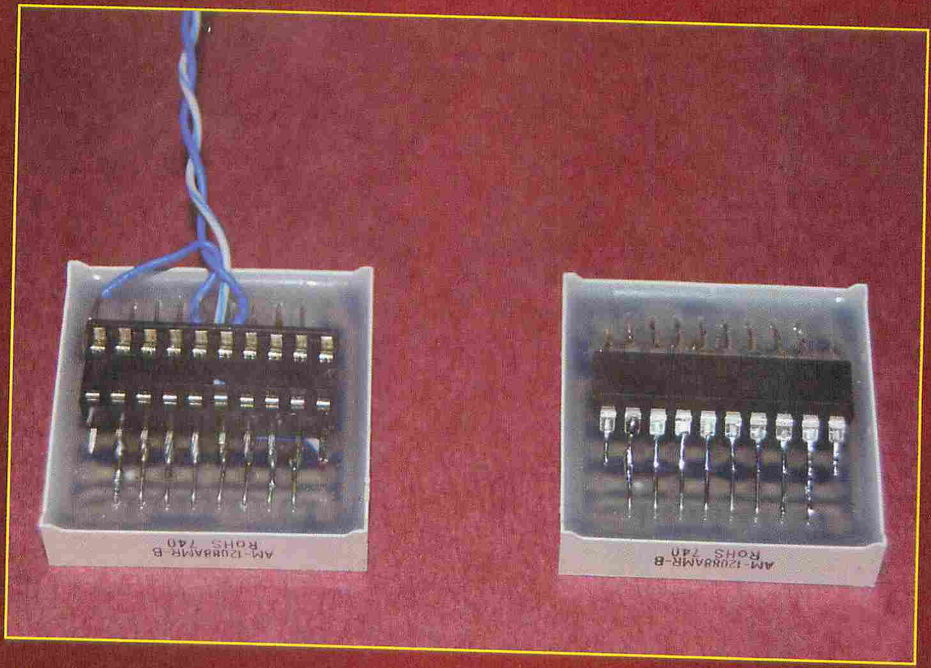
In queste pagine abbiamo solo accennato alle infinite possibilità offerte da questo eccellente software di crittografia, che deve la sua potenza anche ad altri strumenti pronti a gestire, per esempio, crittografie selettive. Il Dataset Editor, tanto per intenderci, consente di pianificare con calma e precisione i file da inserire in un archivio criptato, anche se provengono da cartelle diverse. In più, ricordiamoci che Kryptel offre una grande sicurezza nella fase di codifica: in caso di crash improvvisi del sistema, la procedura è bloccata, senza generare file criptati danneggiati.

L'albero di HackNatale



Con poca spesa, un minimo di manualità e una buona dose di fantasia vediamo come creare decorazioni originali

Pochi componenti assemblati con maestria per creare un'installazione animata di sicuro effetto. Un'idea da regalare e reinventare in diversi modi, da portare in discoteca o da utilizzare come pallina elettronica sotto l'albero oppure perché no, da regalare a molti amici. Costa poco (5-6 euro!), è completamente personalizzabile e non si trova nei negozi.

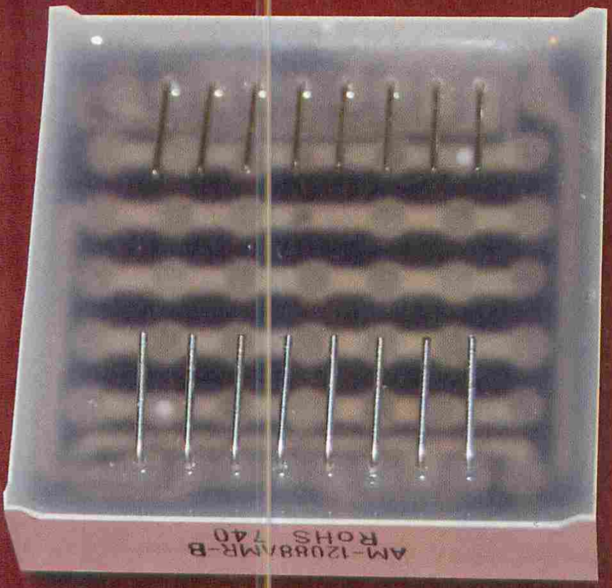


La fase di saldatura è fondamentale, un piccolo errore e tutta la nostra bella teoria va a farsi benedire. Ricordiamoci di fissare il chip durante l'operazione con del nastro adesivo.

Siamo quasi a Natale e come ogni anno non so cosa regalare ai miei amici. Quest'anno però intendo rifarmi e stupire tutti. Donerò ad ognuno di loro una matrice di led sulla quale passano scritte e animazioni personalizzate! Mi costa pochi euro, ci faccio una discreta figura e nel costruirlo mi diverto anche. Sono variati i suoi possibili utilizzi: appeso all'albero, fatto spuntare fuori da una tasca per la serata al locale alternativo, in casa come se fosse un quadro futuristico... per far sapere a tutti di che cosa si circonda un vero geek.

:: Come funziona il sistema?

La matrice mostra immagini e scritte in scorrimento grazie al chip ATtiny2313 che le è saldato dietro. Questo microcontrollore funziona tra i 5.5v e gli 1.8v ed è possibile attivarlo dunque senza problemi con una coppia di batterie AA (scelgo le batterie AAA solo per una questione di eleganza). Una volta accesa la matrice vedremo immagini e scritte scorrere sullo schermo ma il microcontrollore starà accendendo una sola riga alla volta; ciclando tutte le righe molto velocemente il microcontrollore ingannerà il nostro occhio che vedrà un'immagine intera.



Possiamo trovare la matrice di led 8x8 su ebay a meno di 1,50 €

Prima di iniziare è opportuna un'altra premessa. Le animazioni e le scritte che appariranno sulla nostra matrice andranno programmate nel chip ATtiny. Una volta saldato assieme alla matrice non sarà più possibile riprogrammarlo senza rischiare di bruciare tutti i led della matrice stessa (i programmatori di solito lavorano a 5v). Consiglio di costruire la prima matrice animata interponendo un socket da 20pin tra la matrice stessa e il chip ATtiny in modo da poterlo togliere, riprogrammare e reinserire fin tanto che non sarete soddisfatti del lavoro. E' possibile seguire la guida sia che si decida di utilizzare il socket sia che no, è necessario ricordarsi di inserire il socket al posto del processore Attiny2313 e vice versa!

:: Programmare il microprocessore

Per prima cosa è necessario programmare il chip Attiny2313. Prendete il vostro programmatore di eeprom e scrivete il software che vi propongo sul chip. Potete scaricarlo da http://blackman.amicofigo.com/hj/64pixels.zip Assicurativi di aver installato WinAVR (in caso di un computer windows) (http://winavr.sourceforge.net). Vi consiglio di utilizzare la versione 3.4.6 di avr-gcc (WinAVR-20060421--install.exe) poiché produce eseguibili molto compatti. Prima di compilare il codice avrete bisogno di sistemare il file Makefile di 64pixels. Nel mio caso ho impostato la variabile PROGRAMMER a "PROGRAMMER = -c dasa -P COM3 -C C:\WinAVR\bin\avrdude.conf" dove "dasa" è il tipo di programmatore che utilizzo, COM3 è la porta alla quale è attaccato il mio programmatore e

C:\WinAVR\bin\avrdude.conf è dove si trova il file avrdude.conf.

Portatevi nella directory dove avete scompresso il file zip, lanciate "make clean", "make" e quindi "make install" per caricare il software sull'integrato Attiny2313.
Potete anche variare il codice di matrix.c ma per una prima prova è consigliabile utilizzare quello fornito, dato che è sicuramente funzionante!

Alcuni consigli per personalizzare il codice?

I #define iniziali determinano le ripetizioni delle immagini e delle scritte sullo schermo e la loro velocità: impostando questi parametri otterrete i primi semplici cambiamenti

#define ANIMATION_SCROLL_SPEED 80 // velocità di transizione delle animazioni

#define TEXT_SCROLL_SPEED 120 // velocità di transizione del testo
#define REPEAT_ANIMATION 6 // quanto ripetere le animazioni nella modalità ciclo

#define REPEAT_TEXT 3 // quante volte ripetere il testo nella modalità ciclo
#define MAX_MESSAGES 3 // quanti messaggi intendiamo utilizzare (ricordatevi di sistemare anche l'array messages[] in concordanza con MAX_MESSAGES!)

Gli sprite invece sono cosi definiti

```
const prog_uint8_t PROGMEM
sprite_00[] =
 {
   0x18,  // ___XX___
   0x3C,  // __XXXX__
   0x7E,  // _XXXXXX_
   0xDB,  // X_XXXX_X
   0xFF,  // XXXXXXXX
   0x24,  // __X__X__
   0x5A,  // _X_XX_X_
   0xA5   // X_X__X_X
 };
```

e ogni coppia di sprite genera un'animazione! Inventare una nuova animazione è molto semplice. Prendete un quadrato di 8x8 e disegnate per punti il vostro nuovo sprite. Per ogni riga assegnate uno 0 per ogni quadretto vuoto, e un 1 per ogni quadretto pieno e trasformate il valore ottenuto in esadecimale. Nell'esempio riportato ___XX___ indica 00011000 che in esadecimale è appunto 0x18! Non sapete come convertire un numero binario in esadecimale? Google potrebbe aiutarvi. Provate la chiave di ricerca "0b00011000 in hex" ...

:: Costruire la matrice

Costruire la nostra matrice animata è abbastanza semplice. Non ci sono schede perforate da produrre e tutti i componenti (matrice e integrato) vengono saldati direttamente tra loro.
Prendiamo dunque il nostro socket e pieghiamo tutti i pin rivolgendoli verso l'esterno. Per fare questo aiutatevi con una pinzetta e fate in modo che i pin siano bene allineati sia verticalmente sia orizzontalmente tra loro. Questo è un procedimento delicato e andrebbe eseguito correttamente al primo tentativo perché piegare più volte i pin del socket potrebbe provocarne la rottura. Facciamo lo stesso con i pin della matrice piegandoli all'interno. Potreste utilizzare un righello come supporto per la piegatura.

Prendete ora la matrice e guardandola dalla parte dei pin posizionate la parte con la scritta (nel mio caso AM-12088AMR-B)



Un piccolo trucco: per evitare di rompere le saldature èmuovendo la matrice consigliamo di annodare il fili tra i pin della matrice e dell'integrato

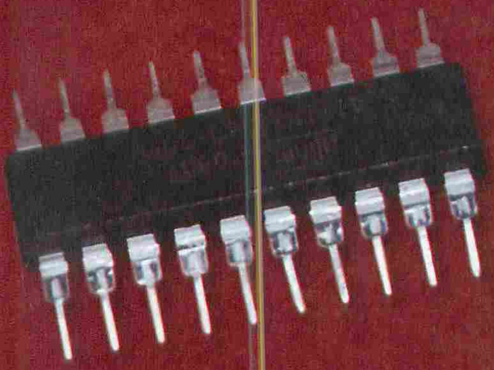
LA LISTA DELLA SPESA

Materiale necessario:

- 1x Matrice di led 8x8 da 3x3cm. (www.ebay.it 1.50€)
- 1x ATtiny2313 (1€)
- 1x Porta batterie per 2 AAA con switch (www.ebay.it 1.50€)
- 2x Pila AAA
- 1x Opzionale – Socket 20pin per ATtiny2313

Materiale per la realizzazione:

- Saldatore, programmatore di eeprom per ATtiny2313.
- Consigliato programmatore USBTinyISP (http://www.ladyada.net/make/usbtinyisp/) tuttavia se possedete un device che può scrivere gli ATtiny, va bene. Io ho utilizzato un Minipov3 (http://www.ladyada.net/make/minipov3/index.html). Tutti i componenti sono molto comuni e probabilmente reperibili presso il negozio sotto casa.



facciamo molta attenzione al corretto allineamento dei pin del socket.

verso il basso. Prendete il chip o il socket e posizionatelo sopra i pin della matrice centrandolo. A destra e a sinistra rimarranno fuori dai contatti 2 pin. L'unghia del chip deve trovarsi a destra. Se avete già programmato il chip, saldatelo! Potete aiutarvi con delle piccole mollette o un pezzetto di nastro adesivo per tenere fermo il chip durante le prime saldature. Ricordate che la saldatura deve essere eseguita in maniera veloce e precisa, per evitare di rovinare il microcontrollore scaldandolo eccessivamente.

HACKING E CARAMELLE

Non sai come presentare il tuo lavoro? Sapevi che progetti di piccole dimensioni come questo possono essere installati all'interno delle più disparate scatolette? Benché esistano in commercio box nati appositamente per contenere lavori di elettronica, un modo simpatico per presentare il proprio lavoro è quello di inscatolarlo dentro confezioni di caramelle! Oltre che dare un tocco di colore e fantasia ricorderai a tutti che che è davvero fatto in casa!



Esistono caramelle diventate famose per la particolarità della confezione; alcune sembrano nate apposta per essere riutilizzate e modificate! Le "Penguin Caffeinated Peppermints" (http://peppermints.com) si distinguono ad esempio per essere vendute in una confezione di alluminio con l'effige di un pinguino (disponibile in quattro colori!). Per la rete circolano piccoli pre-amplificatori installati dentro tali box: non solo potrai gustarti caramelline alla caffeina ma richiamerai anche il tuo amore per il pinguino! Anche le caramelline Altoids (http://www.altoids.com) sono famose per la loro confezione: ben cinque tipi di gusti con altrettante scatoline metalliche colorate e di diverse dimensioni. Il progetto più famoso correlato a queste caramelle? Senza dubbio il MintyBoots: un caricabatterie a pile per iPod e iPhone (http://www.ladyada.net/make/mintyboost).

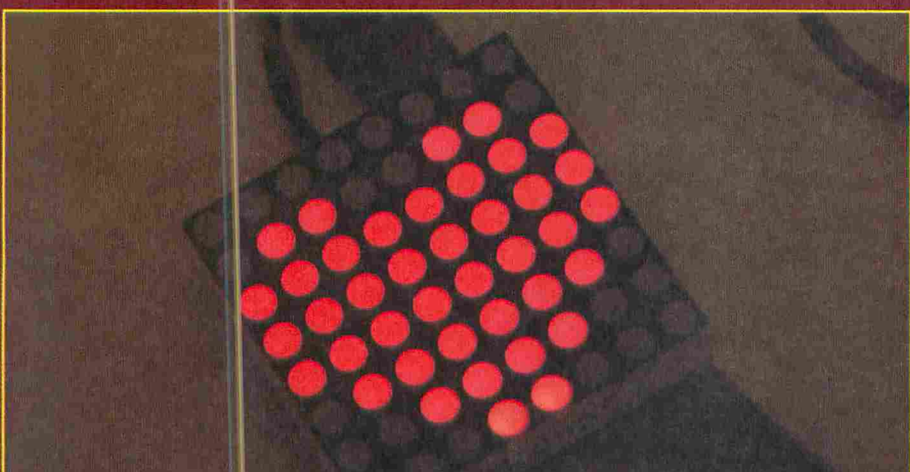
Adesso occorre connettere il porta batterie alla nostra matrice in modo da poterla alimentare correttamente. Saldiamo il filo del negativo (nero) sul primo pin dell'ATtiny2313 libero in alto a sinistra, e il positivo (rosso) sull'ultimo in basso a sinistra. Il modo migliore per evitare di rompere queste saldature muovendo la matrice è quello di annodare i fili tra i pin della matrice e dell'integrato.

Proviamo ad accendere la nostra matrice adesso! Se avete eseguito il procedimento correttamente dovreste iniziare a vedere immagini e scritte scorrere sullo schermo! Volete fare una foto del vostro lavoro? Un trucco che potete utilizzare per fermare le immagini in movimento è quello di collegare il pin 11 (quello che si trova in fronte al filo nero) col pin del negativo (quello dove è collegato il filo nero). In questo modo si ferma l'immagine presente sulla matrice e sarà possibile scattarne una foto.

Se avete utilizzato il codice proposto, provate ad accendere e spegnere più volte la matrice, otterrete ogni volta un messaggio diverso!

Adesso, se avete inserito un socket per l'ATtiny2313 potete toglierlo per riprogrammarlo e provare nuove velocità, scritte o inventare disegni! Non vi resta che personalizzarlo dedicandolo ai vostri amici, che sicuramente invidieranno il vostro ingegno!

Se volete fare una migliore figura vi consiglio di incastonare la matrice all'interno di un altro oggetto, come ad esempio una pallina di natale; se siamo hacker, oltre che creare, qualcosa dovremo pur smontare, no?

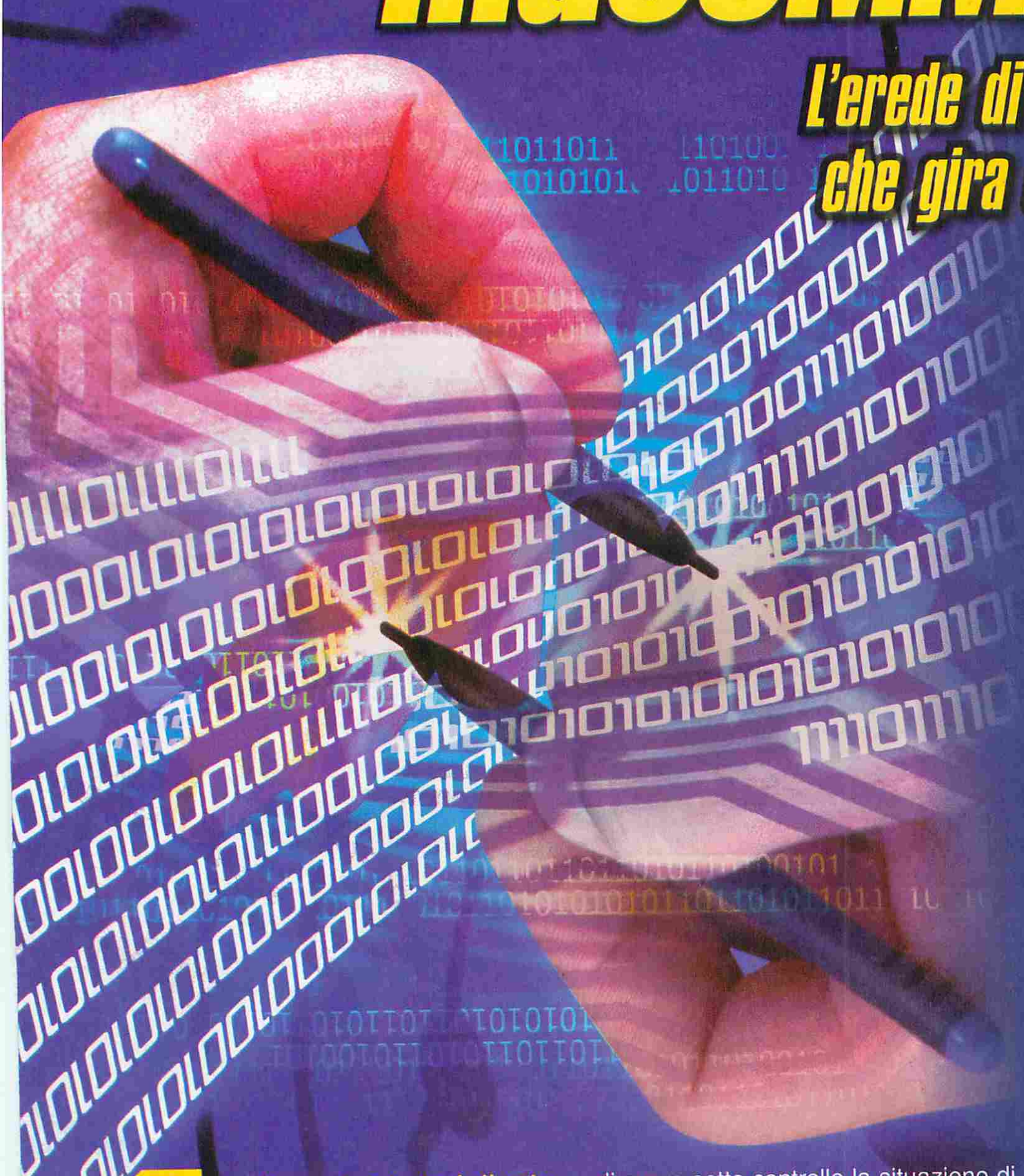


Ed ecco il risultato finale della nostra fatica: un cuore pulsante, il cuore di un hacker.

Federico Galli

muCOMMANDER

L'erede di Norton Commander che gira su ogni piattaforma



Per gli amministratori di rete utilizzare lo scripting è la regola nella gestione dei sistemi, ma a volte fa estremamente piacere avere uno strumento grafico evoluto come muCommander che permette di semplificare e velocizzare molte operazioni.

Il nome ricorderà a molti lo storico Norton Commander (clonato in diverse versioni e per diversi sistemi operativi) di cui mantiene la filosofia basata su due finestre affiancate che permettono di avere sotto controllo la situazione di due cartelle diverse. Ma aggiunge molto di più. La particolarità di muCommander (muC) è quella di essere stato sviluppato con particolare riguardo alle reti, alla leggerezza e alla gestione di diversi formati integrati. Tramite muC si possono infatti compiere operazioni tra due cartelle poste su server diversi, ognuna delle quali può utilizzare anche un diverso protocollo e interconnettere virtualmente piattaforme molto diverse tra loro senza dover usare diversi strumenti.

:: Caratteristiche

muC (www.mucommander.com) è multipiattaforma dato che è stato realizzato in java e completamente opensource. Questo permette di averlo disponibile per praticamente tutti i sistemi operativi: Windows, Linux, MacOS X, FreeBSD, OpenVMS. È inoltre disponibile una versione portabile che contiene al suo interno il solo bytecode java e due starter, per Windows e sistemi Unix, nel caso si voglia provarlo su un sistema senza volerlo installare o per averlo sempre pronto su una propria usb pen.

Per poter lanciare muC è necessario che sul sistema sia installato almeno il Java Runtime Environment 1.4.0 (fornito di base su Mac OS X ad esempio), tuttavia è consigliabile aggiornarsi almeno alla versione 1.6.0 o successive perché le precedenti non preservano gli attributi per i file eseguibili.

muC supporta nativamente diversi formati di archiviatori opensource, come 7z, TAR, GZip, BZip2, ma anche ZIP e RAR. In particolare, per gli ZIP è supportata la modifica "on-the-fly" che permette di effettuare operazioni di aggiornamento sul singolo file senza dover ricomprimere tutto l'archivio permettendo ad esempio di aprire un archivio zip remoto per selezionare un file al suo interno e decomprimerlo altrove. Sono supportati anche i formati binari ISO/NRG, AR/Deb e gli archivi LST.

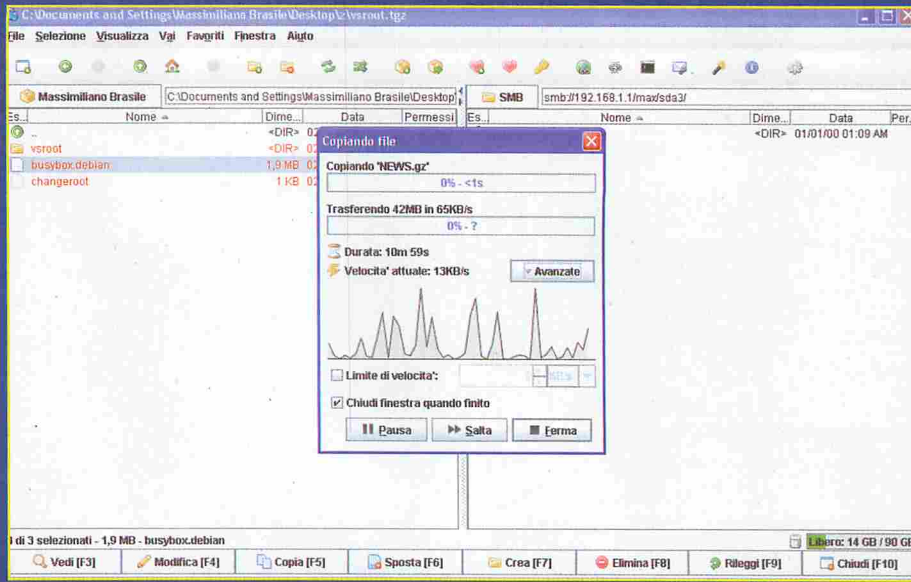
:: Funzionalità

Usare muC permette di avere il massimo controllo sui file a prescindere di dove risiedano, grazie

alla sua capacità di virtualizzare i file system remoti e questo si traduce automaticamente in un risparmio di tempo. I protocolli supportati sono FTP, SFTP, SMB, NFS, HTTP e Bonjour e vengono gestiti come file system virtuali grazie alle due finestre.

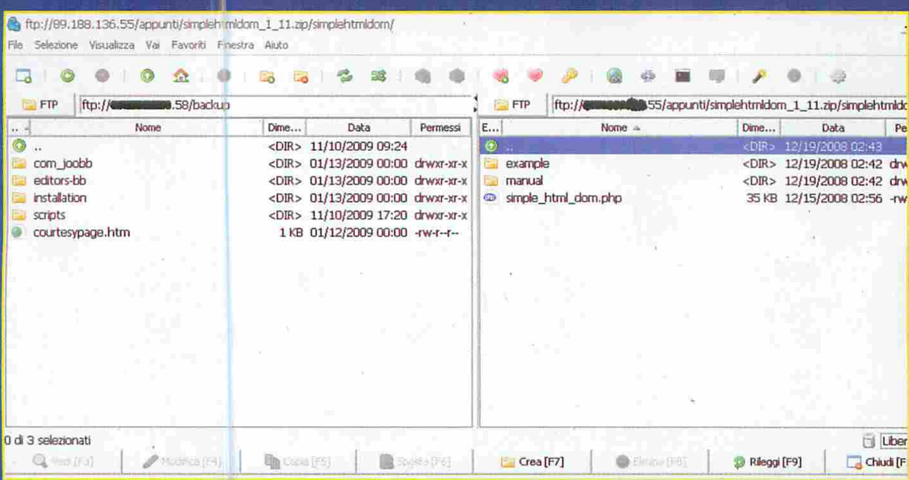
Ho potuto ad esempio sincronizzare una cartella ext2 di un server Linux privo di consolle tramite protocollo samba, con una cartella locale di un pc con Windows, come se avessi avuto le due cartelle fisicamente sullo stesso server e con lo stesso filesystem. Windows non riusciva ad aprire una sessione samba verso il server, probabilmente per problemi legati alle autorizzazioni degli utenti e se avessi collegato fisicamente l'hard-disk del server al pc Windows non avrei potuto leggerlo: Windows non gestisce infatti ext2, a meno di driver terzi e l'alternativa sarebbe stata quindi quella di collegare l'hard-disk del server a un pc con Linux o caricare una distribuzione live sul pc con Windows o direttamente sul server e dopo un paio di reboot avrei potuto concludere. Grazie a muC, senza smontare e installare nulla, non ho dovuto far altro che aprire in una finestra la cartella locale del pc con Windows e nell'altra attivare un collegamento samba verso l'indirizzo del server fornendo i dati dell'utente del server, senza preoccuparmi di toccare la configurazione del pc Windows.

Per verificare la flessibilità del programma ho ripetuto la stessa operazione sincronizzando però cartelle localizzate tra due server ftp distinti entrambi remoti. In questo caso il processo di trasferimento è più lento (il pc con muC diventa il nodo obbligato per entrambi i trasferimenti), ma è notevole osservare come il software riesca a svolgere in modo impeccabile un'operazione che avrebbe richiesto la creazione di un mirror in locale e una successiva sincronizzazione sul server finale.



Samba sulla Vodafone Station non è così user-friendly: grazie a muC il trasferimento dei file diventa invece molto semplice.

Tra le caratteristiche più interessanti vanno poi citati il multi-rename, che permette di selezionare un elenco di file su cui applicare dei filtri per eseguire un'operazione di rinomina di gruppo e anche il supporto nativo per operazioni di divisione (split) e ricombinazione (combine) di file molto grandi, anche questa eseguibile da remoto. È possibile poi chiedere di decomprimere o comprimere da remoto un archivio direttamente nella cartella dove si trova o spedirlo via e-mail come allegato.



Sincronizzare le cartelle tra due server ftp è un'operazione di routine, ma con muC diventa ancora più veloce e a prova di errore.

:: Sviluppi futuri

Il progetto è abbastanza giovane e sono presenti ancora delle mancanze, come il supporto limitato al bookmark, ma la community degli sviluppatori è molto attiva e sono costantemente al lavoro per migliorarlo. Tra gli item in sviluppo per la prossima release sono in programma *l'abbandono* dei Java 1.4, l'inserimento di una funzione di ricerca, il miglioramento del supporto agli archivi RAR. Già l'ultima release al momento disponibile (0.8.4) risulta davvero stabile e user-friendly, supporta 22 lingue tra cui l'italiano ed è altamente personalizzabile, sia come temi e colori, che come visualizzazione dei vari bottoni.

muC rappresenta sicuramente uno strumento di lavoro valido che riesce a colmare con efficienza quel gap legato allo scambio di dati tra sistemi diversi connessi in rete.

Massimiliano Brasile



Dal Regno Unito arriva Internet Eye, un "gioco" che sfrutta sistemi di videosorveglianza per catturare i criminali

Grande Fratello a caccia di ladri

Immaginiamoci la scena: siamo davanti al nostro bel monitor e, tramite una serie di finestre del browser che puntano a delle telecamere di videosorveglianza, scopriamo un ladro che sta commettendo un furto. Clicchiamo subito su un apposito pulsante e... dopo qualche istante, vedremo comparire un messaggio che ci informa che abbiamo appena guadagnato un punto. In capo a qualche ora, poi, i punti guadagnati potrebbero diventare tre, perché la nostra segnalazione ha portato alla scoperta di un crimine.
Un momento: che succede?

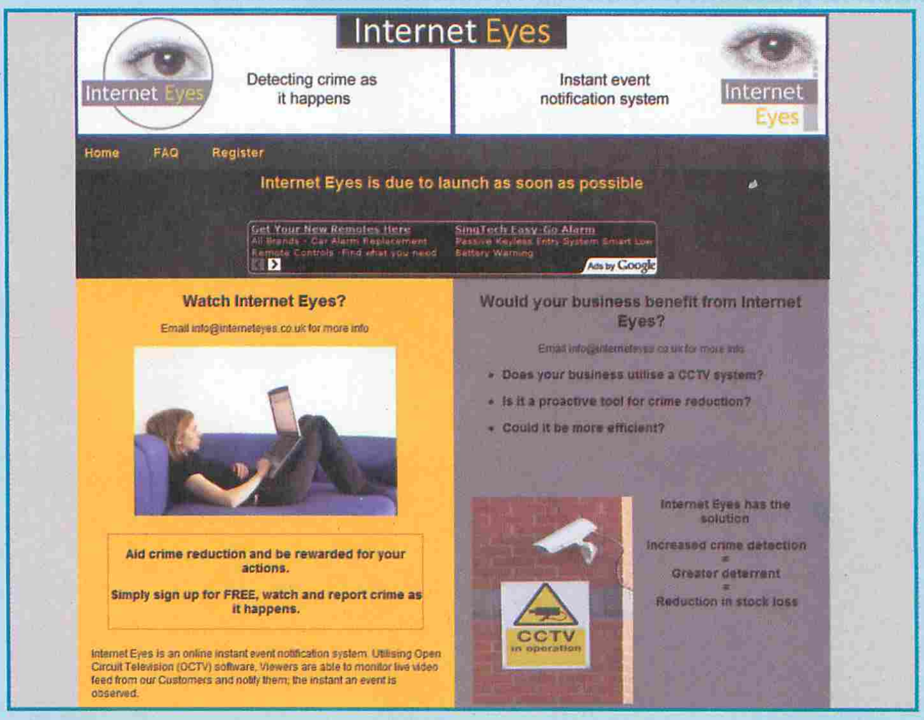
:: Il gioco delle videocamere

Stiamo giocando a Internet Eyes, nuovo servizio web di matrice britannica, destinato a rivoluzionare il mondo della sicurezza e della privacy. Come anticipato, è un vero e proprio gioco, che sfrutta una rete di videocamere di sorveglianza sparpagliate in uffici e locali pubblici della cittadina di Stafford. Iscrivendosi al sito ufficiale, www.interneteyes.co.uk, si ha la possibilità di entrare in partita. A questo punto, basta scegliere quali telecamere osservare e tenersi pronti al clic. Un punto dato per ogni segnalazione, tre punti dati se questa smaschera un malvivente in azione, un punto tolto se invece si rivela inattendibile. Chi guadagna più punti ha diritto al montepremi mensile, che si aggira, spicciolo più spicciolo in meno, intorno ai 1.100 euro.

:: Giocatori e clienti

La registrazione come "giocatore" è gratuita, ma è disponibile anche una sottoscrizione per eventuali "clienti" del servizio. Vale a dire che, se si possiede un locale dotato di sistema di videosorveglianza, ci si può collegare alla rete messa in piedi da Internet Eyes, e dare le riprese

in pasto ai navigatori. Ovviamente, le implicazioni in materia di tutela dei dati personali sono tantissime, e le associazioni di difesa dei diritti dei consumatori sono già scese sul piede di guerra. Di fatto, tramite Internet Eyes è possibile spiare chiunque. I gestori del servizio si difendono, sostenendo che, tuttavia, i giocatori non conoscono a priori la posizione delle telecamere che utilizzano. E poi, vogliamo mettere la sicurezza offerta (sostengono loro)? "è solo una questione di prevenzione del crimine", riferisce James Woodward, fondatore di Internet Eyes. E continua: "Ciò che stiamo facendo è di mettere più occhi possibili su quelle videocamere, in modo da controllare meglio". Charles Farrier, dell'associazione No CCTV, non è affatto d'accordo: "è uno sviluppo disgustoso e preoccupante".



L'home page del sito di Internet Eyes: giocatori o clienti, tutti passano di qua...

:: Le prime impressioni? Mmm...

Ambo le fazioni, comunque, stanno facendo i conti senza l'oste: i primi giudizi su Internet Eyes non sono esattamente lusinghieri. Alcuni giocatori, infatti, lamentano la bassissima qualità delle immagini, senza contare la noia nel dover rimanere incollati ore e ore davanti al monitor, spesso (per fortuna, c'è da dire) senza alcun risultato. Chi invece, sotto sotto, è un grande fan del servizio, è la polizia britannica, che del suo sistema di videosorveglianza, al momento, se ne fa davvero poco. In un rapporto della polizia metropolitana inglese, è emerso che nel 2008 si è risolto, grazie alle videocamere, solo un crimine ogni mille dispositivi installati. Forse è per questo che il Regno Unito è considerato "il regno delle CCTV". Si stima, infatti, che ce ne sia addirittura una ogni 14 abitanti!



Basta un giretto per le strade delle principali città UK per rendersi conto che il "Grande Fratello" ci osserva da ogni angolo.

:: I pericoli sono tutti da valutare

Scherzi a parte, che le autorità inglesi nicchino sulla questione è una realtà, e nessuno sembra preoccuparsi nemmeno di un altro aspetto: la sicurezza informatica. Di fatto, si sa poco o nulla del software che gestisce Internet Eyes, ma è ipotizzabile che un attacco andato a buon fine metterebbe il sistema di CCTV sotto il controllo di un qualsiasi malvivente con qualche abilità informatica. Insomma, un serpente che si mangia la coda.

E la vicenda assume risvolti ancora più inquietanti quando si pensa che, in caso di successo, Internet Eyes sarà esteso a tutto il Regno Unito, per diffondersi su scala mondiale il prossimo anno.

Nel frattempo, il servizio sta raccogliendo le prime pre-registrazioni: basta andare sul sito, cliccare su Register e compilare l'apposito modulo. Al termine della registrazione, non che resta che aspettare l'attivazione, e si è pronti per giocare. Al di là delle considerazioni sulle possibilità di successo di una simile operazione, si aprono scenari fantascientifici su ciò che ci aspetta nei prossimi anni. Città come quelle descritte nello splendido film "Eagle Eye", magari date in mano a sistemi di rilevamento automatizzati, pronti a segnalare abusi, ma anche abitudini della popolazione. E magari adattarsi di conseguenza, sulla base delle volontà di investitori e finanziatori.

A quel punto, la ribellione sarebbe affidata solo a quanti hanno le conoscenze e gli strumenti per combattere il sistema sul piano informatico. Hacker, proprio loro. Ma questa, in fondo, è solo una storia. La realtà di Internet Eyes, al momento, basta e avanza.



Sbirciamo il kernel

Sprofondiamo nei meandri di un sistema operativo e captiamo i suoi meccanismi di gestione dei processi

Il sistema operativo in un computer ordinario è il componente (virtuale) più importante che possa esistere, non solo per l' utente, ma anche per la macchina stessa. Quando accendiamo il nostro pc, subito dopo la fase di boot, il nostro sistema operativo prende le redini di ogni cosa, gestendo una fitta rete di canali di comunicazione tra hardware e software continuamente in attività per andare a creare quello che è agli occhi di un comune utente un ambiente interattivo. Ma quali sono i meccanismi che stanno al di sotto di tutto questo lavoro? E soprattutto, da dove si originano? La risposta sono i processi, gli operai di un enorme cantiere che formano una struttura solida e ordinata. Un processo non è altro che l' astrazione di un programma, o in un linguaggio più semplice, la parte di quest' ultimo che viene eseguito. Per capirne l' importanza, può essere interessante pensare che sui sistemi unix-like, il kernel (il cuore di un sistema operativo) viene eseguito grazie alla chiamata del processo "init", che possiede tutte le informazioni necessarie per il regolare caricamento del sistema.Dopo questa chiamata vengono generati centinaia di sottoprocessi, come il gestore di rete, i driver video e audio, il desktop manager, e tutti i servizi indispensabili ad un ordinario utilizzo della macchina. Una volta che il kernel inizia il suo lavoro, il primo problema a cui si trova di fronte è come gestire una quantità così grande di processi. Il compito non è semplice, perchè bisogna fare in modo che i processi che, come per ogni cosa in un computer sono elaborati dalla cpu, sfruttino al massimo le potenzialità di quest' ultima. Il concetto di base è semplicissimo: rendere il tempo produttivo. Quindi ogni qual volta che un



In questa fase iniziale il processo init carica tutti i servizi di sistema.

CPU <------ Processo 1(100 ms)

Processo 2(5 ms)

Processo 3(10 ms)

Immagine 1: Processo1, che è in attesa, sarà il prossimo ad essere eseguito, seguiranno Processo2 e Processo3.

CPU <-- Processo 4(2ms) Processo 1(3ms) Processo 2(5ms) Processo 3(7ms) <-- Scheduler Processo1(3ms) Processo2(5ms) Processo3(7ms) Processo4(2ms)

Immagine 2: I processi, ordinati dallo scheduler, godranno della cpu in base al loro tempo di esecuzione.

processo in esecuzione non richiede più cpu, verrà sostituito con un altro in attesa. Il kernel del sistema operativo affida questo compito allo scheduler. Sarà proprio lui a mettere in gioco un politica di scheduling (schedulazione) e quindi a decidere quale processo verrà eseguito per primo nella cpu e con quale criterio. Solitamente questo criterio (denominato politica di scheduling) dipende dalle esigenze dell' utente ultimo, ovvero dal tipo di utilizzo che si andrà a fare con la macchina in questione, ma ne esistono comunque diversi generalizzati. Quello che faremo sarà proprio analizzare le regole di schedulazione più importanti che uno scheduler può mettere in atto nel suo lavoro.

:: FCFS

Questo forse è l' algoritmo più semplice da comprendere proprio perchè si riscontra molto spesso nella vita quotidiana. Fcfs è infatti l' acronimo di "First come first served", ovvero il primo processo che richiede l' utilizzo della cpu viene servito. Facciamo l' esempio di un barbiere che può servire una persona alla volta: quando arriva un cliente, questo controllerà se la poltrona sia libera, se è così, verrà servito dal barbiere altrimenti dovrà attendere e far notare ai successivi potenziali clienti che è lui che sarà servito al turno successivo. Riportando questo esempio allo scheduling è facile immaginare come questo comporti una coda di processi, situazione d' altronde inevitabile per ogni altro tipo di algoritmo, proprio perchè la cpu analizza un processo per volta. Il problema sorge però quando un processo richiede molto tempo d' esecuzione e quindi magari potrebbero esistere altri processi che in quel frangente avrebbero potuto essere eseguiti lasciando il posto libero molto prima. Il risultato quindi non è ottimale (Immagine 1).

:: SJF

Dalle conseguenze del Fcfs probabilmente nasce l' algoritmo Sjf, acronimo di "Shortest job first". Attraverso questa politica di scheduling i processi che richiedono meno tempo di utilizzo di cpu verranno serviti per primi. Lo svantaggio quì è che i processi che richiedono molto tempo di utilizzo di cpu potrebbero rimanere in attesa per molto tempo e non è raro il verificarsi delle cosiddette "starvation", ovvero delle situazioni di stallo in cui un processo, non viene mai eseguito. Il risultato è spesso un errore critico del sistema con il suo conseguente blocco. Una domanda spontanea una volta capito questo meccanismo potrebbe essere come sia possibile individuare i tempi di esecuzione di un processo in modo che lo scheduler compia il suo lavoro. Anche qui si arriva ad un altro problema: questo tempo di attesa viene stimato dai programmatori e dai sistemisti e il risultato potrebbe rivelarsi non esatto con consegunze sgradevoli. Un ultimo appunto su questo algoritmo è che se 2 o più processi presentano lo stesso tempo di esecuzione si prenderà in considerazione la soluzione Fcfs (Immagine 2).

:: Priority scheduling

Il Sjf è uno speciale caso del più generale algoritmo a priorità. In questo caso i processi verranno organizzati dallo scheduler in base ad un valore di priorità, portando nella cpu processi a priorità maggiore. E i processi con una priorità molto bassa? Anche in queste situazioni si potrebbero portare *alla luce* condizioni di starvation, ma vi è una soluzione: l' Aging, tramite il quale ad ogni processo viene aumentata la priorità dinamicamente ad ogni intervallo di tempo.

:: Round robin scheduling

Questo algoritmo è disegnato specialmente per i sistemi time sharing, che basano la gestione dei processi in base ad un cosiddetto time quantum. Il concetto è semplice: viene definito un intervallo di tempo (solitamente tra 10 e 100 millisecondi) e i processi, organizzati attraverso la politica Fcfs, godranno della cpu solo per quel frangente di tempo, rimettendosi in coda (se l' esecuzione non è stata completata) una volta scaduto. Osserviamo come le prestazioni di questo algoritmo dipendono principalmente dal time quantum considerato. Se questo sarà molto grande, il risultato apparirà infatti molto simile ad un algoritmo Fcfs, mentre se l' intervallo di tempo sarà molto piccolo si parlerà di "Processor sharing" e apparirà all' utente come se ogni processo avesse un proprio processore a causa dei rapidi cicli di esecuzione (Immagine 3).

Intervallo di tempo 10ms

Processo 1(3ms) <--- CPU <---- Processo1(13ms), Processo2(7ms)

Immagine 3: Se il tempo di esecuzione di un processo è maggiore dell' intervallo considerato, questo dovrà aspettare il suo turno.

Dir31 Dir31@rbt-4.net

Programmare portabile



Scopriamo la potenza e versatilità di MShell

MShell è un linguaggio ad alto livello, con il quale è possibile creare, in modo totalmente gratuito e direttamente sul proprio dispositivo, applicazioni per smart-phone con sistema operativo Symbian S60 (2nd, 3rd e 5th edition). Il linguaggio è organizzato in moduli, tramite il quale è possibile gestire le varie componenti dello smart-phone (messaggi, connettività, grafica, illuminazione, ecc...) e, sin dalla versione 3.0, permette al programmatore di prendere la strada della programmazione strutturata o, a scelta, orientata agli oggetti, fornendo un pratico sistema per la creazione di classi. Un tipico codice mShell inizia sempre con l'inclusione dei moduli che verranno usati nel corso del programma, secondo la sintassi use modulo1, modulo2. I moduli sono fondamentali in mShell poiché permettono di svolgere tutte le operazioni base sui componenti dello smart-phone tramite le funzioni e le variabili contenuti al loro interno. Altra importante caratteristica del linguaggio è l'assenza di un tipo "esplicito" per le variabili: nessuna variabile è infatti intrinsecamente di un determinato tipo, ma ogni variabile può assumere un diverso tipo in base al valore che a questa viene assegnato.

:: Classi e istanze

È chiara l'importanza delle classi nel mondo della programmazione ad alto livello e quanto la loro esistenza aiuti il programmatore nello sviluppo di applicazioni, per tutti i motivi di riusabilità, di leggibilità e di mantenimento che le circondano. Aldilà dell'esempio banale mShell permette ai programmatori di creare velocemente classi di diverse dimensioni e di diversa complessità.

:: Il modulo UI

Uno dei moduli più importanti messi a disposizione da mShell è il modulo



L'immagine mostra lo stesso codice eseguito su tre diversi smart-phone con diversi sistemi operativi. E' facile portare lo stesso programma su smart-phone diversi!

STRAPPO 1

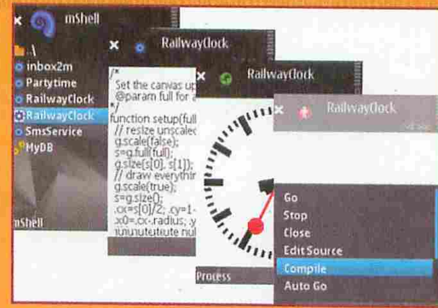
```
class ProvaClasse      //creazione di una classe
  varA;
  varB;

  function init(val1, val2=5)     //costruttore della classe
    this.varA=v1;
    this.varB=v2;
  end;

  function somma_prodotto(param)
    return (this.varA+this.varB)*param;
  end;
end;

nomeOggetto: ProvaClasse = ProvaClasse(val1, val2);    //
creazione di un oggetto
nomeOggetto.varA=5;
nomeOggetto.somma_prodotto(valore);
```

UI (User Interface) che fornisce funzioni per la creazione e visualizzazione dei menu, delle finestre di dialogo e per l'interazione col dispositivo. Cercheremo di dare qui una breve spiegazione dell'utilità di alcune delle funzioni contenute in questo modulo. Innanzitutto è possibile personalizzare nelle proprie applicazioni il menu che appare premendo il tasto di selezione sinistro, ed è buona norma sostituire quello di default con un menu personalizzato. E' possibile far questo tramite la funzione ui.menu, per mezzo della quale si attribuisce un nome al tasto e si definisce un nuovo menu. ui.list permette la creazione di una utilissima lista di elementi selezionabili dall'utente. I parametri da passare alla funzione sono essenzialmente: il vettore degli elementi, un booleano che indica la possibilità di selezionare più di un elemento, e gli indici degli elementi preselezionati. La funzione restituisce infine un vettore contenente gli indici degli elementi selezionati. Nelle tante applicazioni realizzabili sarà certamente necessario ottenere degli input dagli utenti, di tipo testuale o numerico, che permettano il naturale proseguimento dell'applicazione. Per permettere a un utente di interagire con l'applicazione una importante funzione è la ui.query, che visualizza una finestra di dialogo per l'inserimento di un input da parte dell'utente. I parametri richiesti dalla funzione sono: il testo interno alla finestra, il titolo della finestra e il valore iniziale della casella di testo (in base alla quale verrà determinato il tipo del valore di ritorno della funzione). Un comportamento simile è ottenibile con la ui.form, con la differenza che in questo caso è possibile inserire da un'unica finestra diversi valori, i quali vengono poi ritornati sotto forma di array. La funzione che di certo risulta più utile per l'interazione con il dispositivo, e alla quale è necessario prestare particolare attenzione è la ui.cmd, il quale scopo principale è quello di riconoscere la pressione di un tasto o il "tocco sullo schermo". Proprio in base a questa fondamentale differenza tra i dispositivi si rende necessario un diverso approccio all'utilizzo di questa funzione! Nei dispositivi "non touchscreen" (in generale 2nd e 3rd edition) è necessario far precedere la funzione ui.cmd dalla ui.keys, tramite la quale si dichiara l'interesse all'utilizzo degli eventi tastiera. Il valore ritornato dalla funzione ui.cmd per questi dispositivi è un vettore contenente i codici dei tasti premuti. Nei dispositivi "touchscreen", i quali non sempre sono forniti di tastiera, è invece necessario richiamare dapprima la funzione ui.ptr, con la quale si dichiara l'interesse verso gli eventi del cursore. Per questi dispositivi la ui.cmd ritornerà un vettore di 3 celle contenente, in ordine, la coordinata orizzontale, la coordinata verticale e l'evento (pressione o rilascio). L'unico parametro, tra l'altro opzionale, da passare alla funzione ui.cmd è il tempo, in millisecondi, per il quale il dispositivo dovrà attendere. Se a tale funzione non viene passato alcun parametro questa attenderà per un tempo indefinito che accada un evento. Altre due funzioni interessanti, per le quali vale la pena spendere qualche ultima parola, sono ui.confirm e ui.error. La prima mostra una finestra di dialogo per richiedere la conferma dell'esecuzione di un determinato evento e ritorna true o false a seconda che la richiesta venga accettata o rifiutata; la seconda simula una finestra di errore contenente il testo passato come parametro.



Alcuni esempi di istruzioni eseguite su un Nokia N95 (Symbian S60 3rd edition).

STRAPPO 2

```
ui.menu("Menu", ["Rosso", "Verde", "Blu", "Esci"], false);
ui.list(["Mela","Pera","Banana"], false, []);
ui.query("Inserisci il tuo nome:", "Dati personali", "");
ui.form(["Nome":"", "Cognome":"", "Età":0]);
ui.confirm("Vuoi veramente uscire?","Domanda");
ui.error("Questa è una finestra d'errore!");
ui.keys(true);
tasto=ui.cmd(1000);
ui.ptr(ui.relative);
coordinate=ui.cmd(1000);
```

:: Curiosi?

Speriamo con questo articolo di aver attirato la vostra curiosità! mShell offre la possibilità di creare piccole e grandi applicazioni con un codice molto semplice e intuitivo, ma la potenzialità più grande sta proprio nel continuo aggiornamento che ad esso viene fornito! Del resto il mondo di mShell è ben più grande di quel che può entrare in un articolo e ci vorrebbe forse un libro per descriverlo in maniera più dettagliata. Con queste istruzioni potete però già iniziare a smanettare col linguaggio!

Massimo Milazzo